SEE PAGE 15!

WIN! LG 34in MONITOR

apc

Dec 2015
Issue 422

YOUR EXPERT TECH

THE BEST FREE SECURITY APPS

BUILD A COMPLETE SECURITY SUITE FOR FREE!

THE NO-BS PLAIN ENGLISH GUIDE!

MAKE A FAIL-SAFE WINDOWS BACKUP

DON'T GET CAUGHT OUT: FOLLOW OUR STEP-BY-STEP BACKUP PLAN

DIGITAL PRIVACY & SECURITY

REVEALED: WHAT THE REAL THREATS ARE + HOW TO PROTECT YOURSELF ON *ALL* YOUR DEVICES

HOTTEST TECH REVIEWED

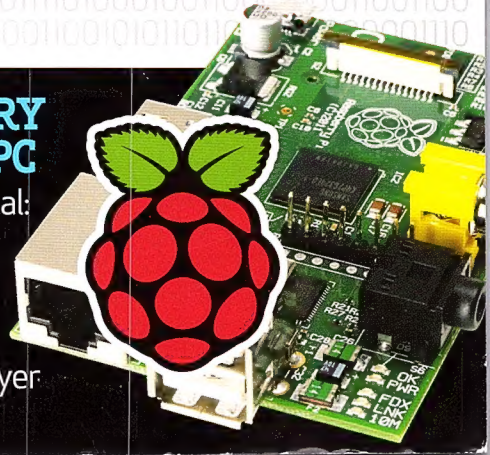
- ASUS's ultimate gaming monitor
- Pocket keyboards
- The amazing printer with 2-year ink tanks
- Apple iPad mini 4

SECURITY APPS & SERVICES

- VPN subscriptions: who's got your back?
- Password managers: safe and easy to use
- Android security apps: why you need one

RASPBERRY PI MEDIA PC

In-depth tutorial: Build & customise a powerful, flexible & low-cost media player



Future

IEEE 802.11ac Wireless and VoIP Solution for NBN (and non-NBN) Home and Business Networking

DrayTek Aust & NZ
www.draytek.com.au

NBN Ready | UFB Ready | 32x VPN

Vigor2860ac / Vigor2860Vac
VDSL2/ADSL2+ & Gigabit WAN Router

- Multi-WAN with VDSL2/ADSL2+, Gigabit Ethernet WAN and USB ports for 3G/4G dongles
- Six Gigabit LAN ports with multiple subnets and 50,000 NAT sessions
- Two USB ports for 3G/4G USB modems, network printer, storage and USB thermometer
- Integrated IEEE 802.11ac wireless Access Point; dual band; up to 1300Mbps throughput
- VoIP (2 x FXS and 1 x FXO Line Port) for Vigor2860Vac

NBN Ready | UFB Ready | 50x VPN

Vigor2925ac / Vigor2925Vac
Dual Gigabit WAN Broadband Router

- Multi-WAN with dual Gigabit Ethernet WAN and USB ports for 3G/4G dongles
- Five Gigabit LAN ports with multiple subnets and 50,000 NAT sessions
- Two USB ports for 3G/4G USB modems, network printer, storage and USB thermometer
- Integrated IEEE 802.11ac wireless Access Point; dual band; up to 1300Mbps throughput
- VoIP (2 x FXS and 1 x FXO Line Port) for Vigor2925Vac

NBN Ready | UFB Ready | 2x VPN

Vigor2132ac
Gigabit WAN Broadband Router

- Integrated IEEE 802.11ac wireless Access Point; dual band; up to 1300Mbps throughput
- 1 x Gigabit Ethernet WAN interface with security object-oriented SPI firewall and QoS
- 4 x Gigabit Ethernet LAN ports with 30,000 NAT sessions
- 2 x USB ports for USB printer, storage and USB thermometer

TAIWAN EXCELLENCE 2015

VigorAP 910C
802.11ac Ceiling Mount Wireless Access Point

- IEEE 802.11ac wireless Access Point with PoE PD port and ceiling mount housing
- Supports multiple SSID with bandwidth management per SSID
- Equipped with advanced central wireless management (AP Management)
- Up to 866Mbps Wi-Fi throughput

i-LAN TECHNOLOGY

i-LAN Technology Pty Ltd trading as DrayTek Aust & NZ
www.i-lan.com.au (02) 9838 8899 sales@i-lan.com.au

© Copyright December 2015 i-LAN Technology Pty Ltd. All rights reserved.

apc

Future Publishing Australia,
PO Box 1077, Mount Street, North Sydney, NSW 2059
Tel: 02 9955 2677 Fax: 02 9955 2688
SUBSCRIPTION ENQUIRIES: Please call Magshop 13 61 16
Email: apcmag@futurenet.com
Web: www.apcmag.com

EDITORIAL
Editor-in-Chief **Dan Gardiner**
Senior Journalist **Paul Taylor**
Senior Journalist **Shaun Prescott**
Journalist **Joel Burgess**
Journalist **Stephen Lambrechts**
Sub-Editor **Carmel Sealey**

ART/PRODUCTION
Creative Director **Troy Coleman**
Senior Designer **Nykke Coleman**
Designer **Sharnee Brisbourne**

CONTRIBUTORS
Keith Andrew, Alice Bell, Jonni Bidwell, Helen Bradley, Nathan Brown, Alex Campbell, Simon Chester, Simon Crisp, Alan Dexter, Ian Evenden, Craig Grannell, Ben Griffin, Christian Hall, Lindsay Handmer, Leon Hurley, Paul Lilly, Ashton Mills, Jenneth Orantia, Nick Peers, Matthew Pellett, Les Pounder, Matthew JC. Powell, Alun Pughe, James Robinson, Mayank Sharma, Alan Stonebridge, Zak Storey, Nathan Taylor, Luis Villazon, Jarred Walton, Darren Yates

SENIOR MANAGEMENT
Chief Operating Officer **Neville Daniels**

COMMERCIAL
Sales Director Paul Marttila
paul.marttila@futurenet.com

ABOUT THE MAGAZINE
APC is published by Future Publishing Australia.

Distributed in Australia and NZ by Network Services.

Printed by Webstar
All contents copyright Future Publishing (Overseas) Ltd, trading as Future Publishing Australia copyright 2013. All rights reserved. While all care is take to ensure information is correct, please check prices and specifications before purchase.

PRIVACY STATEMENT
This issue of APC published by Future Publishing Australia may contain offers, competitions or surveys which require you to provide information about yourself if you choose to enter them or take part in them (Reader Offer). If you provide information about yourself to Future Publishing Australia, Future Publishing Australia will use this information to provide you with products or services you have requested, and may supply your information to contractors to enable Future Publishing Australia to do this. Future Publishing Australia will also use your information to inform you of other Future Publishing Australia publications, products, services and events. Future Publishing Australia may also give your information to organisations that are providing special prizes or offers and are clearly associated with the Reader Offer. Unless you tell us not to, Future Publishing Australia may give your information to other organisations that may use it to inform you of other products, services or events to give to other organisations that may use it for this purpose. If you would like to gain access to the information Future Publishing Australia holds about you please contact Future Publishing Australia's Privacy Officer.

Future

ABOUT FUTURE
Future Publishing Australia is part of Future plc. Future produces carefully targeted special-interest magazines, websites, and events for people who share a passion. We aim to satisfy that passion by creating titles offering value for money, reliable information, smart buying advice, and which are a pleasure to read or visit. Today we publish more than 180 magazines, websites and events, with over 100 international editions of our magazines published under license in 30 countries around the world. Future plc is a public company quoted on the London Stock Exchange (symbol: FUTR)

Peter Allen Chairman of the Board
Zillah Byng-Thorne Chief Executive Officer

FIPP

Extra items for your security toolkit

APC's editor details some of his favourite online security and privacy tools.

The threats to our digital security and privacy have arguably never been worse, but thankfully there's a range of tools, techniques and services that can help minimise the risks. We've outlined a heap of those in this month's cover stories, but inevitably some of our favourites didn't fit neatly into a particular feature. As such, I thought I'd commander this month's editorial to list some of the items in my personal security toolkit:

- Protect yourself on public Wi-Fi – Hotspot Shield Free VPN Proxy (**tinyurl.com/apc422-hots**).

While it's not as fast as paying for a dedicated VPN subscription service (which will route all your internet traffic through a secure server) this Chrome plugin is a good no-cost option for keeping you safe on free Wi-Fi hotspots, which are basically the networking equivalent of a public bath. (Trust us: you don't want to know what's floating around in there.) It can also spoof your location so that you appear in, say, the US, so you can use locale-specific video streaming services.

- Stop web trackers – Privacy Badger (**www.eff.org/privacybadger**).

This browser plugin for Firefox and Chrome blocks online ad-systems and other intrusive cookies from tracking your movements online. Be aware that it can break some website layouts, so if you suddenly find that your favourite site isn't displaying properly, you may need to disable it.

- Sign out of (almost) all web sites – Super Logout (**superlogout.com**).

If you're often using shared or public computers, this site aims to take the pain out of logging out of everything before you leave. Be warned that just visiting this site is basically the nuclear option when it comes to logging out. As soon as you hit the URL, it'll send logout requests to every site it supports – which numbers in the dozens. If you want to try it out, we'd strongly suggest not using your main web browser – use an alternate like Internet Explorer.

- Deactivate and close accounts – Just Delete Me (**justdelete.me**).

Shutting down accounts for sites you no longer use – or that you don't like the privacy policies of – can be a painful experience. This site will take some of the hurt out, with direct links to the account-cancellation page of a huge variety of major sites and services. These are also handily ranked by difficulty, from Easy to Impossible, so you can anticipate how much trouble you're in for.

- General security and privacy apps and services – Prism Break (**prism-break.org**).

If you're looking to replace insecure and/or intrusive services with better alternatives, check out the big list of options at Prism Break, which breaks down apps and services by platform. ■

DAN GARDINER
EDITOR-IN-CHIEF
dan.gardiner@futurenet.com

Contents

Issue 422 December 2015

37

DIGITAL PRIVACY & SECURITY

REVEALED: WHAT THE REAL THREATS ARE + HOW TO PROTECT YOURSELF ON *ALL* YOUR DEVICES

68

30 YEARS OF FREE SOFTWARE

JONNI BIDWELL DELVES INTO THE ORIGINS OF FREE SOFTWARE AND REMINDS US THAT MUCH OF TODAY'S SOFTWARE FREEDOM IS DUE TO THE EFFORTS OF A SINGLE, HAIRY HACKER.

» features

37 DIGITAL PRIVACY & SECURITY: THE NO-BS SUPERGUIDE
Revealed: what the real threats are + how to protect yourself on all your devices

68 30 YEARS OF FREE SOFTWARE
Jonni Bidwell delves into the origins of free software and reminds us that much of today's software freedom is due to the efforts of a single, hairy hacker.

» technotes

06 NEWS
The latest developments in the tech world.

08 NUMBER CRUNCH
The numbers behind the big tech news.

10 GADGETS
Hot tech gear we want to own.

12 HOW IT'S DONE
GoPro Hero4 Session

14 EPINIONS
See what *APC's* readers are talking about.

16 END USER
Not everything is plain sailing in the tech world.

"Some readers are no doubt ready to gently point out, "Mate, see that little black dot on the back of your phone? It's called a 'camera', you boofhead!" Turn your Android into a video monitor, P90

27 MOTOROLA MOTO G

25 ASUS STRIX-GTX950 DC2OC-2GD5-GAMING

23 ASUS PG279Q

26 ZAGG POCKET KEYBOARD

25 GIGABYTE GV-N950XTREME-2GD

20 SAMSUNG 950 PRO 256GB

» the lab

18 LATEST REVIEWS

18 HP ZBook 14 G2
19 Apple iPad mini 4
20 Samsung 950 Pro 256GB
22 Asustor AS5002T
23 ASUS PG279Q
24 Epson Workforce ET-4550
25 ASUS STRIX-GTX950-DC2OC-2GD5-GAMING
25 Gigabyte GV-N950XTREME-2GD
26 Zagg Pocket Keyboard
26 Microsoft Universal Foldable Keyboard
27 Motorola Moto G (2015)
28 Samsung Galaxy Note 5
28 Oppo R7 Plus

30 SOFTWARE REVIEWS

30 Windows software
31 Apple Mac software
32 Linux apps
33 iOS App Store
34 Google Play (Android)
35 Windows Phone apps

» how to

72 QUICK TIPS

We fix readers' computing problems.

74 TUTORIALS

74 Stay notified in Windows 10
77 Create and format sparklines in Excel VBA
78 Make a fail-safe Windows backup
84 Unlocking El Capitan's not-quite-Siri
86 Create custom vibrations for iPhone
88 Back up a drive in Linux

92 MASTERCLASSES

92 PC Builder: New life for an old PC
96 Raspberry Pi: Create a Pi-powered media PC
100 Android: Turn your Android into a video monitor
104 Arduino: Arduino Wi-Fi – Part 1
106 Coding: Claiming your inheritance

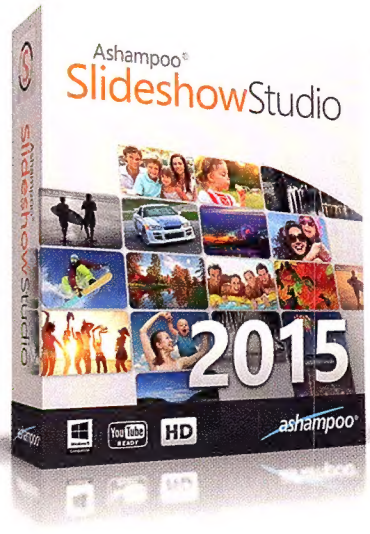
» downtime

110 GAMES

High-performance playtime.

114 CHIP CHAT

News from the world of geekdom.



» on the disc

- **Ashampoo Slideshow Studio**
- **5 Great Safety Tools for Windows**
  LastPass
  AVG Free AntiVirus
  WinPatrol
  Sophos Virus Removal Tool
  ISpy Connect
- **5 Essential Media Apps**
  Darkwave Studio
  Foobar2000
  GIMP
  Rename Master
  Audiograbber

Find your disc inside on page 83. (Australian edition only.)

Controversial Australian data-retention laws now in effect

But major ISPs warn they're not ready to implement them yet.

It's official – as of October 13, Australia's telecommunications companies are required by law to start storing two years worth of your private metadata logs. That means that every text message or email you send, every phone call you make or receive, as well as your IP address, will be logged and filed on servers at your telco for two years.

Though the actual content of your phone calls will not be stored, your location during those calls will be recorded, as well as the duration of the conversation, and the identities and locations of both parties on the either end of the phone line.

The same goes for the content in your emails, and while the websites you visit will not be stored, your IP address will be kept on file so that law enforcement can track unlawful activity back to you – it's kind of like giving the police your fingerprint records before any crime has been committed.

Government bodies are now able to access this private information without your permission and potentially even without a warrant. Questions also linger over which specific bodies will have access to the data, whether it will be stored here or off-shore and how it will be encrypted.

Though Australia has only just implemented the data retention legislation, several countries in the European Union have already abandoned similar metadata laws after having been ruled unconstitutional.

Other countries with data retention laws generally only hold on to the metadata for around six months to a year, unlike the two years in Australia's version of the bill. Opponents of the scheme say that this poses a greater risk to individual privacy and security.

Though Australia's ISPs have had six months to prepare for the data retention scheme, 84% of them have stated that they're not ready to implement the measures necessary, with two-thirds of them still unsure as to what type of metadata they're supposed to keep. The Attorney-General's department now says telcos have until April 2017 to be compliant.

Stephen Lambrechts

A Trans-Pacific sucker punch?

Copyright holders awarded more rights in secret new trade agreement.

The battle between copyright holders and pirates is about to get even more intense, according to new documents released by WikiLeaks. The controversial, secret-spilling organisation has leaked what's purported to be a near-final version of the Trans-Pacific Partnership (TPP) deal that Australia recently signed. The leaked agreement, titled 'TPP Treaty: Intellectual Property Rights Chapter', awards Hollywood studios the right to go after pirates directly and sue them.

It states that ISPs will be forced to hand over infringers' contact details and would also have to keep track of serial pirates and narc on them.

How much would pirates have to fork out? That much is unclear, however the document states that the "amount that would be sufficient to compensate the right holder for the harm caused by the infringement, and with a view to deterring future infringements."

We know what you're thinking — doesn't each country have its own laws for this sort of thing already? Well, the agreement suggests that each country change its laws to conform with the terms of the TPP. Whether that will actually happen is, at present, an open question.

Stephen Lambrechts

Goodbye Windows Control Panel?

Future versions of Windows 10 may ditch the 20-year-old core feature.

After decades of faithful service, Microsoft will be retiring the iconic Control Panel section of its Windows operating system, carrying its functionality over to Settings, which will become the default application for changing your PC's settings in upcoming builds of Windows 10. The two applications have lived side by side since Windows 8, acting as a thorn in the sides of confused Windows users. **Stephen Lambrechts**

Musk's Apple smackdown

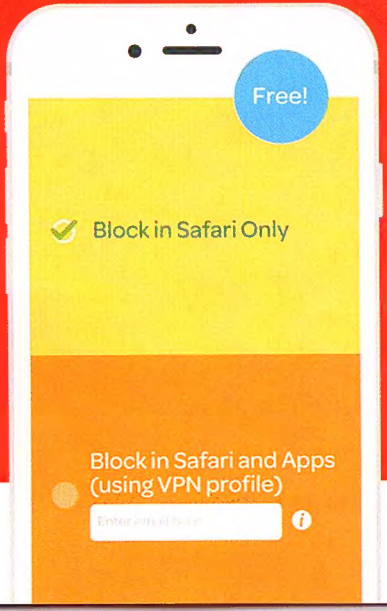
Tesla Motors CEO says Apple's only re-hiring its 'worst' engineers.

Tesla Motors CEO Elon Musk hasn't got much love for Apple – when asked about Apple's plans for an electric car and its hiring of ex-Tesla engineers, Musk told the German newspaper *Handelsblatt* that "they have hired people we've fired," further stating that "we always jokingly call Apple the 'Tesla Graveyard.' If you don't make it at Tesla, you go work at Apple. I'm not kidding." **Stephen Lambrechts**

iOS 9's ad-blocking oops

Apple forced to remove blockers that may compromise OS security.

Though iOS ad-blockers have only recently made their way to Apple's App Store, the Cupertino company has already removed several of them. It was found that some apps would install a root certificate to examine data at a packet level, giving their developers the ability to view a user's encrypted traffic. Apple is now working with these devs to bring their apps back to the App Store. **Stephen Lambrechts**



Router virus seems to fight the good fight

Great—you have a virus!

Cyber criminals are beginning to take an increased interest in home routers and the Internet of Things market as a whole. It's not that there's a lot of personal data on such devices – it's the allure of controlling all these gadgets that's attractive, especially when plotting a distributed denial-of-service attack. However, a newly discovered virus that's taken up residence on thousands of routers may have your welfare in mind.

Security firm Symantec is calling the virus Linux.Wifatch (or just Wifatch). It came to light in 2014, when a security researcher noticed unusual activity on his home router. He discovered a sophisticated piece of code that turned his router into a zombie connected to a P2P network of infected devices. Symantec did some digging of its own and found that much of Wifatch's code is in Perl. It targets several architectures and ships its own static Perl interpreter to each. Once a device is infected, it connects to a P2P network that distributes threat updates.

"The further we dug into Wifatch's code, the more we had the feeling that there was something unusual about this threat. For all intents and purposes, it appeared like the author was trying to secure infected devices instead of using them for malicious activities," Symantec explains.

Symantec hasn't found any evidence to suggest Wifatch is shipping payloads for malicious purposes. Just the opposite—it appears that Wifatch is making routers more secure, by blocking outside hacks and attempting to remove any malware it finds.

So it appears there's a vigilante hacker. However, Symantec notes that Wifatch is still being installed without consent. It also contains backdoors that the author could use for malicious purposes, if desired. **Paul Lilly**

Microsoft seeks to calm Windows 10 privacy concerns

A little clarification goes a long way?

After copping a significant amount of flak regarding its privacy policies surrounding the release of Windows 10, Microsoft has published a set of detailed articles explaining exactly what those policies consist of.

"Windows 10 collects information so the product will work better for you," said the Redmond company to its customers, further stating that it wants to ensure that Windows 10 users "are in control with the ability to determine what information is collected."

Microsoft went on to explain that the collected data, which is encrypted and stored in secure facilities, "doesn't include any of your content or files," and that it has taken "several steps to avoid collecting any information that directly identifies you, such as your name, email address or account ID."

Regarding Personalisation Data, Microsoft also promises that only trivial information is collected, such as "knowing whether you are a Seattle Seahawks fan or Real Madrid fan, in order to give you updates on game scores or recommend apps you might enjoy." **Stephen Lambrechts**

US$67,000,000,000

THE AMOUNT DELL PAID FOR IT GIANT EMC.

Although this figure isn't as big as AOL's purchase of Time Warner in 2000, Dell's recent $67 billion purchase of data-storage outfit EMC still rates as a ridiculous amount of money — and places it as the second-largest acquisition in the tech space ever. Though the offer will remain on the table for 60 days in case another company wants to put in a bid, the other main contender, Hewlett-Packard, is preoccupied with its own internal restructuring, so it's unlikely to make a counter-offer. **JB**

US$862,400,000

THE AMOUNT APPLE COULD OWE A UNIVERSITY FOR IP THEFT.

In October, a US jury found Apple guilty of unlawfully using technology copyrighted by the University of Wisconsin. The patent is for a system that improves processor efficiency, and was developed back in 1998. The university's licensing arm accused Apple of appropriating it for use in its ARM-based A7, A8 and A8X chips. Although specific damages are yet to be finalised, the presiding judge said Apple could be liable for up to US$862.4 million. **JB**

5.6 MILLION

THE NUMBER OF US OFFICIALS WHOSE IDENTITIES WERE REVEALED IN HACK.

If your passwords or bank account numbers are stolen by cyber criminals it can be a considerable ordeal to change them, but if hackers manage to nab unchangeable biometric identifiers like fingerprints, you've got a much bigger problem. Though the hack on the US Office of Personnel Management — responsible for the nation's database of government officials and civil servants — has been widely reported on since June, in September the agency confirmed that the hack was even worse than expected, with records of over 5.6 million employee fingerprints among the data stolen, including many from individuals with intelligence or military security-clearances. **JB**

8.6%

THE PERCENTAGE OF ITS STAFF THAT TWITTER WILL LAY OFF.

After another year of monetary losses and slowing growth, Twitter announced in October that Jack Dorsey (interim CEO for the prior four months and co-founder of the company) will once again officially take the helm of the company. Quick to make changes, Dorsey announced that he would let 336 of Twitter's 4,100 employees go, in an effort to be a leaner company that could respond with faster application iterations. **JB**

97K

HOW MANY DIESEL-POWERED VEHICLES VW IS VOLUNTARILY RECALLING IN AUSTRALIA AFTER IT WAS CAUGHT CHEATING IN EMISSIONS TESTS.

Volkswagen's admission of globally rigging over 11 million cars to artificially report lower emissions during test conditions has understandably angered customers. The anger extends beyond drivers thinking they owned a more economical vehicle, but more broadly, it also means that the company has added an extra 1 million tons of greenhouse gasses and pollution to the world's atmosphere. This is approximately equivalent to the collective yearly emissions of all the power stations across the United Kingdom. 97,000 VW, Skoda and Audi vehicles have been recalled in Aus for having the dodgy tech. That's a Vee-dub mis-step. **JB**

ASRock®

FATAL1TY GAMING GEAR

GET THE GEAR USED BY THE PROS

FATAL1TY 100 SERIES GAMING MOTHERBOARDS

ALTECH COMPUTERS
www.altech.com.au

ACHIEVA GROUP OF COMPANIES
www.achieva.com.au

INGRAM MICRO® Partner Smart

NSW

ARC Computers	02 9748 8322	arc.com.au
Aus PC Market	02 9646 8000	auspc.com.au
Capitol Computer	02 9281 8890	capitolcomputer.com.au
IIBuy	02 9599 0698	iibuy.com.au
IJK	02 9745 0877	ijk.com.au
Megaware Computer	02 9698 1593	megaware.com.au
MSY	02 9755 0668	msy.com.au
mWave	1300 727 446	mwave.com.au
Nexcom	02 4721 3457	dcomponline.com.au
North Shore Computers	02 9939 1548	nscom.com.au
PC Lan	02 9649 3288	pclan.com.au
PC Meal	02 9746 7886	pcmeal.com.au
D & D COMPUTER TECH.	02 9742 3988	ddcomputer.com.au
DIY COMPUTERS	02 9897 9993	diycomputers.com.au
MAIG PTY LTD.	02 9648 2261	maig.com.au
J&W	02 8090 3332	jw.com.au

QLD

Computer Alliance Pty Ltd	07 3420 3200	computeralliance.com.au
Game Dude Pty Ltd	07 3387 1500	gamedude.com.au
MSY	07 3290 1738	msy.com.au
Umart Online	07 3369 3928	umart.com.au
AUSCOMP COMPUTERS	07 3722 5100	auscompcomputers.com

VIC

Computers & Parts Land	03 8542 8688	cpl.net.au
MSY Technology	03 9560 2288	msy.com.au
PC Case Gear	03 9551 0889	pccasegear.com
Centre Com Sunshine PTY	03 8311 7600	centrecom.com.au
Scorpion Tech. Computers	03 8561 3200	scorptec.com.au

NT

PC Solutions 4 U	08 89412119	pcsolutions4u.com.au

TAS

WA

Austin Computer	08 9201 2788	austin.net.au
MSY	08 9344 1002	msy.com.au
Netway Computers	08 9332 0888	netwaycomputers.com
Netplus Micro Computers	08 9242 7288	netplus.com.au
PC West	08 6398 4813	pcwest.com.au
PLE Computers	08 9309 4771	ple.com.au
Worldwide Net Solutions	08 9375 9666	netsolution.com.au
ARROW COMPUTERS	08 9258 7733	arrowcomputers.com.au

SA

Hypernet Computer Distribution	08 8340 2021	hypernetdist.com.au
MATS Systems	08 8186 2110	mats-systems.com.au
MSY Technology (SA) Pty Ltd	08 8212 1656	msy.com.au
IT&Computers	08 8186 2736	itwarehouse.com.au
Photech Computers Pty Ltd	08 8349 4334	photech.com.au

www.asrock.com
FATAL1TY.COM

- The specification is subject to change without notice.
- The brand and product names are trademarks of their respective companies.
- Any configuration other than original product specification is not guaranteed.
- The Fatal1ty name, Fatal1ty logos and the Fatal1ty likeness are registered trademarks of Fatal1ty, Inc., and are used under license. © 2014 Fatal1ty, Inc. All rights reserved. All other trademarks are the property of their respective owners.

technotes

» GEAR WE WANT

KAISER BAAS REVO GLIDER

$800 | KAISERBAAS.COM

According to Kaiser Baas, the Revo Glider is just the first of many 'handleless' Segway-like scooters that it's planning to roll out. With computer-assisted balance and two powerful motors, the Revo will let you comfortably accelerate to 12km/h and the battery should be able to take you around 20km on a single charge. Available in the lead up to Christmas, the Glider looks like it might take a little getting used to when it comes to control... although we suspect that once you get the hang of it, you'll start to consider walking as one of those archaic 'labour-intensive' practices that people used to do when they didn't know any better. **JB**

LIGHT L16

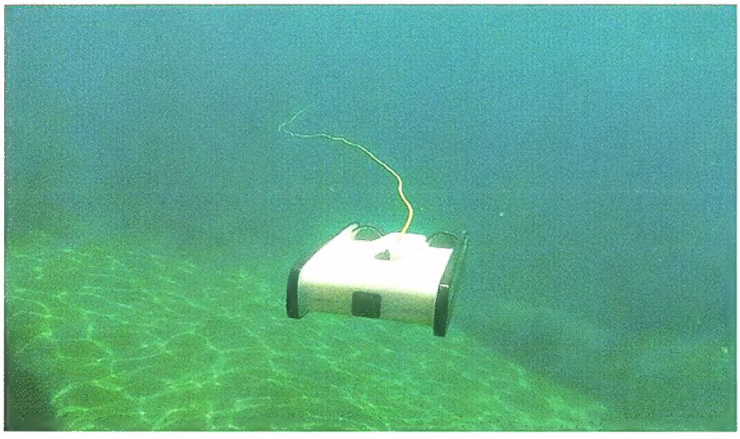
US$1,299 | LIGHT.CO

Historically, photographers have really needed an SLR to take striking photographs in a range of different circumstances – at least if you wanted the resulting images to be high-quality enough to use for print or other professional purposes. But one company has caught onto the fact that this limitation is largely because cameras, to date, have only used a single lens. Thus, it's planning on changing the game with a brand new digital camera called the L16, which (as the name alludes) packs 16 lenses into one neat package that's not much bigger than your average smartphone. Ten of these lenses can fire simultaneously for any one photo, which each capturing at different focal lengths, speeds and with varying apertures. The resulting ten images are then all stitched together on the fly inside the camera, giving you a final image that can be up to 56-megapixels in size. **JB**

OPENROV TRIDENT

US$1,199 | OPENROV.COM

It's fair to say that modern man has a fascination with recording every single thing he can and can't see. But unless you're A) an exceptional free diver or B) James Cameron, you're only going to get fleeting glimpses of life underwater on your action cam. Not anymore. The Trident is a stable underwater vessel that's controlled by a smartphone, tablet or even Oculus Rift from the surface, boasting vertical travel with no pitch and zippy acceleration. The creators say that piloting the Trident is more like flying, and with a 25m tether at the end of a Wi-Fi buoy, you'll be able to get into some fascinating nooks and crannies. **PT**



SHARP LV-85001

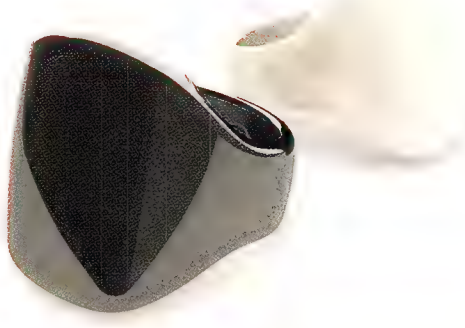
¥16M (~AU$186,000) | WWW.SHARP.NET.AU

4K TVs are so last year. If you really want to be at the bleeding edge of display technology, you'll need to go a bit better than that. Just as well, then, that Sharp has announced that it's working on an 85-inch 8K TV with an IGZO panel that will set you back a cool $186,000. Suddenly that 5K iMac screen doesn't seem so impressive... although you'd need a serious TV cabinet to house this one! High resolution displays are developing at an astonishing rate, with previously impressive resolutions moving further and further down the scale. But do we need 8K? Is it even practical? Probably not, but we're geeks, so it's already given us sweaty palms and heart palpitations. No word yet on when this one will actually see the light of day internationally, but it'll be available in Japan from early November 2015.

DOBOT

FROM US$499 | DOBOT.CC

The Dobot is the robot arm for everyone (that we never knew we needed)! Its makers claim a whole range of uses for it: designing and building products, feeding pets, teaching children calligraphy and more. And it's supposed to be remarkably accurate for such an affordable device, with a measly error margin of about 0.2mm. Although its creators insist it's a tool for everyone, we feel this one's best suited to small businesses and crafters – the type of people who need a high-precision device in their daily business life. But at its relatively low price, it's a marvel that the designers have crammed as much into the Dobot as they have. It's out in December 2015.



OURA

US$299 | OURARING.COM

Oura's makers describe it somewhat inelegantly as a "ring-sized wellness computer", but that's actually a pretty accurate description. It's designed to take all kinds of measurements – from your heart rate and temperature to your sleep quality and activity intensity – and then analyse the info and feed it back to you to suggest ways to improve your lifestyle. What's most appealing about this is that, compared to other activity trackers, it's relatively subtle and unobtrusive, but beneath its modest exterior lies a plethora of high tech smarts. If it can help you sleep and work better, then it could indeed be the one ring to rule them all... ■

GoPro Hero4 Session

Waterproof — until you break the seal.

About iFixit

iFixit is a global community of tinkerers dedicated to helping people fix things through free online repair manuals and teardowns. iFixit believes that everyone has the right to maintain and repair their own products. To learn more, visit **www.ifixit.com**.

BACKGROUND

Surf's up! The new GoPro Hero4 Session just dropped in and it's totally tubular. It's GoPro's first waterproof camera that doesn't require a case. But will the sealants on this Session keep it far from a 10 on our repairability scale? Grab your board because this teardown is about to hang 10!

MAJOR TECH SPECS

- Rugged waterproof design
- 1,030mAh rechargeable lithium-ion battery
- Built-in Wi-Fi, micro-USB, and microSD slot (which is expandable up to 64GB)
- Video capture 1440p at 30fps, and 1080p at 60fps
- 8MP-wide field of view stills

KEY FINDINGS

- It looks like we have our work cut out. Look, a batch of T4 Torx screws on the front! You had us worried for a second there, GoPro. Screws out, and the lens cover comes free, revealing access to an o-ring. The glass lens cover is probably the most likely part to break on the Session, but it's also the easiest to replace. It's good to see that GoPro had repairability in mind for the lens cover. Strange that it sells a complete lens cover-replacement kit...
- After savaging most of the exterior, we aren't surprised to find the GoPro's battery soldered to the motherboard and glued into a bracket. No more removable batteries — presumably in the interest of waterproofing. With an estimated two-hour battery life, you're going to be recharging often, increasing the number of charge cycles on your camera, and decreasing its life before you need to, but can't, replace the battery.
- With a flick of the wrist goes the display and the power/capture button — everything a user needs to operate the GoPro on one confusing bracket. Like everything else, these components are smaller, and feature more complex, intertwined cables than in models past.
- Just like the Hero4 cameras that came before, the Session features an f/2.8 glass lens with an "ultra wide-angle field of view with reduced distortion." Let's hope the waterproofing protection really works — it'll be pretty much impossible to replace this lens without destroying your camera.
- The 8MP sensor drops the 4K capability found in the Hero4 Black/Silver 12MP sensors, instead supporting resolutions up to 1440p at 30fps.
- Repairability Score: 1 out of 10 (10 is easiest to repair). The front bezel is held in place with T4 Torx screws and is easily replaceable. Accessing the device for internal repairs means ripping through a rubber band, plastic casing, and lots of glue, making reassembly infeasible. The inner components are assembled in a web of circuitry and adhesive. ■

GIGABYTE™

G1 GAMING

WORLD of TANKS

ROLL OUT

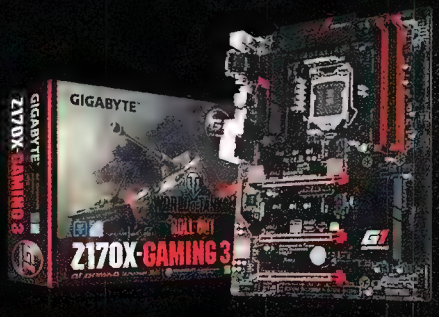
BATTLE READY

intel CHIPSET Z170 inside

SUPPORTS intel CORE inside

GIGABYTE Gaming Series Motherboard | WARGAMING.NET LET'S BATTLE

© 2015 Wargaming.net



GET FREE WORLD OF TANKS PREMIUM

Buy a GIGABYTE Z170X-Gaming 3/5/7 Motherboard

www.gigabyte.com.au

gigabyte.wg-event.com

tech notes
EPINIONS

THE LINUX COMMAND LINE MYTH

I have been using Linux for many years and have never used the command line. It's the same for my friends. I actually find Linux easier to use than Windows – it's simple and easy to install, plus it works like a dream. I wonder though, why does almost every story about Linux have 'command line this and command line that'. The average person does not ever need to touch the command line. That was Linux about 10 years ago.

It seems you wish to make Linux appear hard to use. I have nine Windows machines and they cause me more problems than Linux Mint or Knoppix or Puppy or Hanthana. Windows 8 was a nightmare and I don't think Windows 10 will be any better. So can we see a story about the ease of use and install of Linux? Try running Windows off a USB key, or try installing Window in less than 15 minutes. I can do both with Linux.

Allan Clark

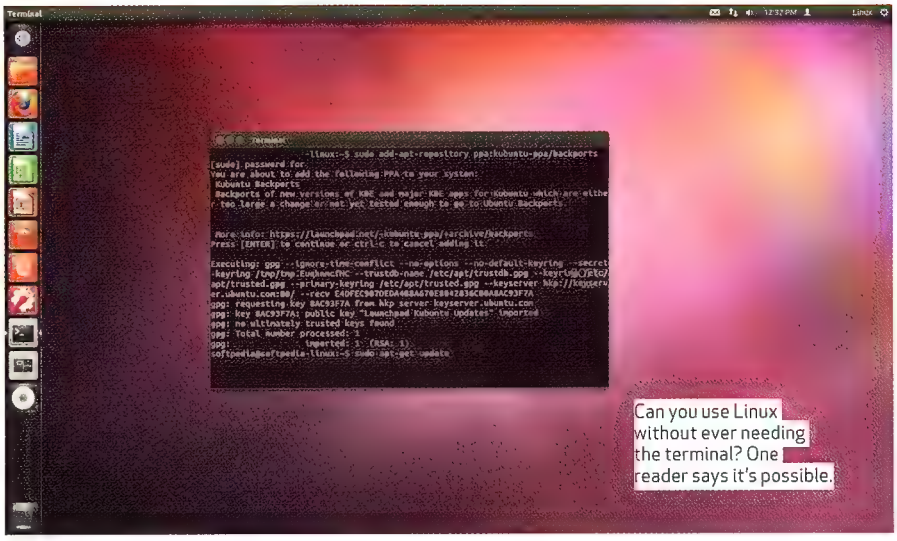
Ed replies: **We've actually run numerous stories in *APC* showing how easy it is to install and use Linux over the years, including a sizable one last year. The more intricate topics we cover in our monthly how-tos often do require a little command-line tinkering, though that's by no means a hard and fast rule. But yes, it's definitely worth re-iterating that you can run Linux without ever having to open the terminal!**

A WINDOWS DEFENDER

I have tried several different devices and OSs but have found that nothing can replace Windows. Android and iOS devices are more portable and sometimes easier to use, but they're not as versatile as devices with Windows. Linux is too hard for the novice to use and the programs are not as polished as Windows programs.

Now you can get tablets with Windows 10 that are portable, can handle all types of media content, are compatible with most external peripheral devices and can be connected to an external keyboard and monitor for use as replacement desktop. Windows is more relevant than ever, not less as stated in your October issue. There have always been devices that are better at doing a particular function, but if you need a device that does everything, nothing beats a device with a Windows OS.

Carl Francis


Can you use Linux without ever needing the terminal? One reader says it's possible.

OLD WINDOWS KEY AFTER UPGRADE TO 10?

Hello guys, great mag – have one query. I had Windows 7 installed on my old PC – it's maybe 4 years old and does my emails, social media and communications work, but no gaming . So I updated to Windows 10 with no problems except for my Bluetooth MX5000 keyboard, which only worked every second or third boot – I've since plugged in a USB one and all's OK.

My question is now whether my old Window s 7 disc is no longer required? Can I sell it with the licence key, or reinstall it on a second computer legally?

And as a follow-up, when I build a new computer to upgrade to, can I install the Windows 10 copy I downloaded onto it legally (since I removed the old copy from my upgraded unit). I know I can download the ISO from Microsoft & create a USB boot disk or DVD, but I have no activation key to install it.

Do I have to purchase a serial key for the new unit? Or can I get the serial key from the old installed unit with a key finder and be able to use that one?

Steven Mew

Ed replies: **You won't be able to legally re-use or resell your Windows 7 key, as you're still technically making use of the licence it provides with your Windows 10 install.**

On the topic of transferring your Windows 10 license to a new PC, this'll also prove somewhat problematic — when you upgrade from an older copy of Windows to version 10, you're not actually issued with a new key. Instead, the device's hardware configuration is given a unique ID that's OKed with Microsoft's activation servers.

If you upgraded select components within your current PC — swapping out the motherboard and CPU, for example — this'd likely deactivate your Windows 10 install. Now, you might be able to get Microsoft to re-activate the system for you, but from what we've heard this is handled on a case-by-case basis and could require some time arguing your case with Microsoft support.

WHERE'S MY MEDIA CENTER, MICROSOFT?

It has become evident that Windows Media Center can be installed on Windows 10 (if not legally, then at least

APCMAG@FUTURENET.COM

Come on, have your say!

We want to hear what you think. Add to these discussions or email your views (in fewer than 250 words) to **apcmag@futurenet.com**. All correspondence becomes the property of *APC* and is subject to editing. Letters must include full name, street address, suburb, state and phone number to be considered for print publication. Address and phone details will not be published.

"You won't be able to legally re-use or resell your Windows 7 key, as you're still technically making use of the licence it provides with your Windows 10 install."

fairly easily) and it works without any problems. So you have to wonder why Microsoft didn't offer it themselves, either in Windows 10, or as an optional extra at a small charge. Even if only 1% of Windows users bought it, that'd be tens of millions of dollars additional income from a product that costs them nothing extra in development costs to sell for Windows 10.

Sure, most Windows users don't use it, but a significant number of loyal enthusiastic users think it's the best product of its type on the market. Microsoft has annoyed the hell out of them, and damaged a whole industry segment that makes products to watch TV on Windows.

Gordon Drennan

IN DEFENCE OF AD BLOCKING

Regarding the November 2015 editorial (see page 3), I have to note that there are legitimate defensive uses for ad blockers.

More and more, we're seeing ads and ad networks becoming malware distribution vectors (and very effective ones give that infected ads can appear on otherwise clean sites). Since there's no way to tell a clean ad from an infected one, and since there's no way to tell if a particular ad network will become infected, ad blockers are increasingly being used as a defensive mechanism to head off this attack vector (particularly in enterprise scenarios). This is in addition to the tracking and annoyance issues that were mentioned in the editorial (particularly the mobile site ad redirects which I've seen far too often).

In any event, ad blockers will be here to stay for the foreseeable future.

Dean Rosolen

SLOW USB DRIVES?

Recently, I was a little frustrated at how slow it was to write a file to a particular USB drive and decided to investigate a little more formally. I have three 16GB drives – two identical Verbatims and one Lexar. (All are formatted as NTFS – the slow Verbatin was just re-formatted).

I wrote an identical file to all three drives and have attached a file showing screen shots of the Windows 8.1 progress bars. (They are pretty neat aren't they?)

Not only do the speeds vary dramatically – from 5.13 to 12MB/s – but the speed patterns through the whole transfer are also quite different. Do you think this data indicates any of the drives is faulty? Do you think these patterns are normal otherwise?

Ed replies: **It's common for different brands and models of USB drives to perform quite differently, so we'd be surprised if you saw the same speeds across all three drives. That said, the two identical Verbatims should perform about the same — at least if they're about the same age and have had similar usage. Flash drive performance does decrease with age, however, so if one of those Verbatim units has seen more reads and writes, that could be why it's slower. The other possibility is that one of them is a a counterfeit — auction sites are littered with fake USB drives, so we only ever buy ours from reputable vendors.** ■

Win!

AN LG 34UM67

This month, we're giving readers the chance to win one of LG's brand new 34UM67 ultra-widescreen, high-framerate gaming monitors.

The LG 34UM67 is a top-notch 34-inch display that picked up an APC Recommended award in last-month's gaming screens comparison. (See APC November, page 59.) It's primed for *buttery-smooth* gaming, with a high-quality IPS panel, 144Hz refresh rate, 2,560 x 1,080-pixel resolution, AMD FreeSync support and built-in stereo speakers.

To enter, head to the competition web page at **tinyurl.com/apc422-comp** and, in 25 words or less, give us your most creative answer to the question:

'If you could make anything you own buttery smooth, what would it be and why?'

This competition is open to Australian and New Zealand residents only. Entries close 30/12/2015. For full terms and conditions see the competition web page.

Backdoors in software: terrible idea, or just a really awful one?

Shaun Prescott weighs in on a feature that governments love to pressure developers for, but that's bad news for consumer privacy.

According to their advocates, when used as intended, security backdoors in software and services are important failsafes: in the event that, say, you end up being a mass murderer or something, they're designed to bypass any encryption or other security measures that might prevent authorities from catching you. Nevertheless, most Western governments' attempts to legislate them into law have been met with consternation – and it's not hard to see why. Apart from the usual concerns about privacy and surveillance, they might not be that safe. After all, if the government and related authorities are capable of accessing your data via a backdoor, what's stopping hackers from doing it whenever the hell they please? Not much, it turns out.

Take South Korea for example. In April, the government passed a new law requiring people under 19 years of age to have monitoring software installed on their smartphones. Among the government-approved programs was an app called Smart Sheriff, but according to research initiated by the Open Technology Fund, the software turned user data into a smorgasbord for identity theft. A report in the *Houston Chronicle* claims phone numbers, browsing history and other data was being sent via the app across the internet unencrypted. Worse still, the app could be hijacked and made to send false alerts to the parents of the teenagers.

Whether these risks are apparent to the Obama government or not is uncertain, but a spokesperson for the White House indicated in October that it will relent on its increased push for security backdoors. For a long time, the US administration's been intent on introducing legislation which would force tech companies to provide backdoor access, but spokesperson Mark Stroh announced the change in tack to media last month. Presumably, the government has finally listened to security experts and resolved that these measures cause more problems than they solve. And that's not even factoring the vastly different approaches each government might take: who's to say China and North America will treat data with the same degree of respect?

Can user rights go too far?

We're all for citizens rights, but a recent court decision in Italy has us scratching our heads.

There's a lot you can't get away with in the modern workplace, or at least, that's what conventional wisdom tells us. You can't watch the *Star Wars* trilogy at your desk, and you can't crack a bottle of wine while perusing the figures. In Italy though, it looks like masturbation is now totally acceptable. That's according to a court ruling in October concerning a sacking at car manufacturer Fiat. The former employee – known only as Giuseppe Z – was caught watching a porno DVD in an electrical supply room on work premises. Once dismissed from his position he took Fiat to court, and won. The Italian Supreme Court of Cassation ruled that Fiat did not reserve the right to sack a worker due to "just a glimpse of the film during a meal break." Take a moment to let that sink in: in the most catholic country on Earth, home to the pope and Vatican, you can now watch porn at your desk. We're living in a strange future. What's next?

ENDUSER

Share your stories!

If you have an iteresting story about technology users, their experiences and the issues that affect us all (whether funny or serious), email us at **apcmag@futurenet.com**. All correspondence becomes the property of *APC* and is subject to editing. Letters must include writer's full name, street address, suburb, state and phone number to be considered for print publication. Address and phone details will not be published.

BLACKBOOK 13 ZERO

COMING SOON

VENOMCOMPUTERS.COM.AU

LAPTOP

FROM $2,049; AS TESTED, $3,500 | WWW.HP.COM/AU

apc RECOMMENDS

HP ZBook 14 G2

The belle of the mobile workstation ball.

At just 1.71kg and 21mm tall, the ZBook 14 doesn't feel like a mobile workstation. In order to make it so light, HP relied heavily on a matted black aluminium upper panel, bordered along the edges with rubber and magnesium. This gorgeous design is perfect for a serious no-nonsense machine.

The bottom panel is mostly black magnesium, save for four rubber feet that keep the laptop steady on all sorts of surfaces and angles. With one button-click, we removed the bottom panel to gain access to an easily removable battery. More tech-savvy users will love the removable panel, as it gives you easy access to the cooling fan, your processors, as well as your wireless card – should you need to quickly upgrade or replace a damaged item.

Despite a thick, unattractive border around the display, the 1,920 x 1,080p screen is bright and colourful. It produces vibrant colours with plenty of detail from a wide range of viewing angles.

There is a touchscreen available, but it's an optional upgrade only, and the laptop won't perform any bends and twists. To be clear, what you're getting with the standard ZBook 14 G2 is a laptop whose screen can bend back 130-degrees, but can't be operated with a finger or stylus.

The standard keyboard base is primarily composed of black aluminium. The backlit keys are made of magnesium and they sit above an aluminium trackpad with two upper and two lower buttons.

HP insist on including the buttons, despite the fact most of us are touch-oriented and scroll and click using only our fingers and a screen on the majority of our personal devices. Although these buttons are superfluous, they don't detract from the ZBook's overall aesthetic.

Although the ZBook isn't the fastest mobile workstation in its ranks, it's not a slouch either. It's got a lot of great features under the hood, enough to put it just below elite company in the mobile workstation class. Packing a fifth-generation Intel Core i7 processor and 16GB of RAM, the HP ZBook 14 G2 isn't messing around in terms of under-the-hood performance. If you're a designer or a video editor, you'll love the elite AMD FirePro M4150 chip, which isn't the most powerful on the market, but the GPU provides enough giddy-up to get the job done while also considering battery drain.

What you won't love about this laptop is its measly 256GB of SSD storage, though you do get a secondary 1TB 7200rpm hard drive, which does help cover your more conventional storage needs.

We were able to run the machine for 11 hours without over-exerting it and it lasted for about 7 hours and 15 minutes playing a film on a loop (at 50% screen brightness and 50% volume).

When we pushed the machine with more than a dozen spreadsheets open and YouTube running in the background, we witnessed no lag in performance and were able to switch between tasks instantly. However, the laptop only lasted about 6 hours and 45 minutes – which is still pretty good for a mobile workstation.

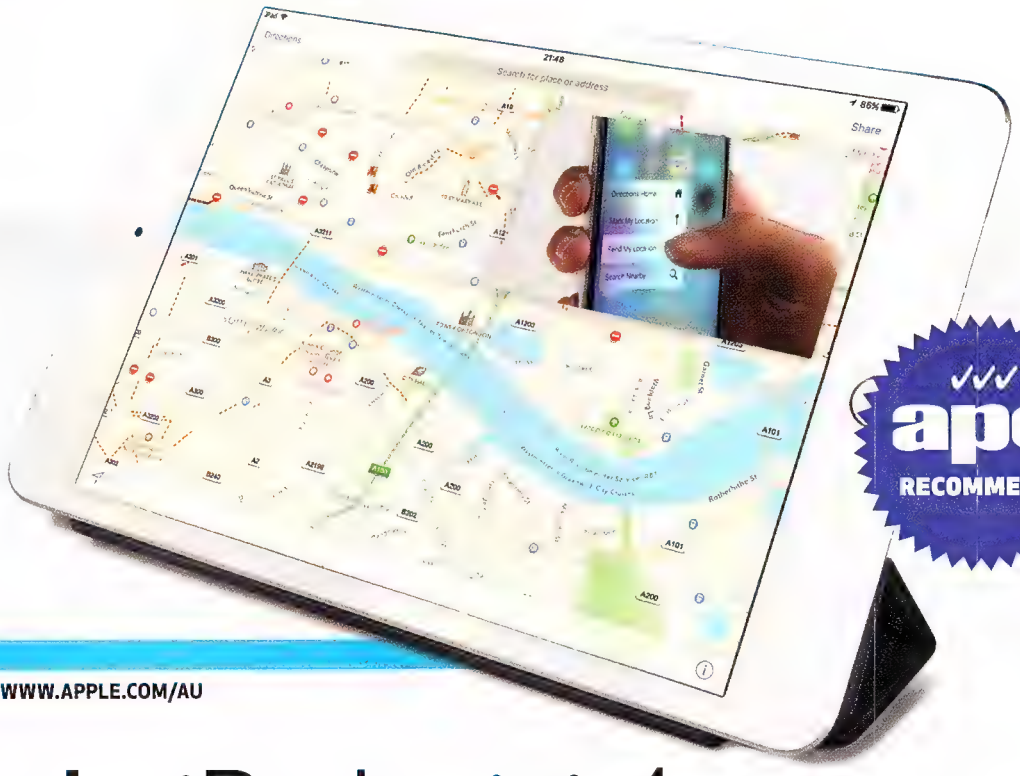
The HP ZBook 14 G2 is the belle of the mobile workstation ball. It's got the looks. It's got the small form factor. And it balances portability and style.

Verdict

Features ★★★½☆
Performance ★★★★½
Value ★★★★☆

If you require strong performance, but you're also concerned about heft and style, this is a fine device.

★★★★☆



apc RECOMMENDS

TABLET

FROM $569 | WWW.APPLE.COM/AU

Apple iPad mini 4

iOS 9 helps make the little iPad big news once again.

Last year's iPad mini 3 was a weak upgrade compared to the Retina iPad mini 2. Its addition of Touch ID only wouldn't have been such a blow if it wasn't for the iPad Air 2 getting an all-round upgrade. The original Air and iPad mini 2 were identical apart from form factor, so the mini 3 felt like a backwards step while the Air 2 leapt forward. Apple has corrected the line-up, giving us the mini we wanted last year, but actually at a time that's more suitable.

Why? It's all to do with iOS 9. Having the iPad Air 2 as the only iOS device capable of using the new system's Split View and Picture in Picture modes (it'll be joined by the iPad Pro in November) didn't make sense. Those new iOS 9 features are big updates that iPad users will really want to use. The new mini has similar guts to the iPad Air 2 (with some cosmetic changes) and it shows off iOS 9 in all its glory. This is one very fast iPad, and even though the tech is a year old, it took serious engineering to rework it to fit in this diminutive housing.

Apple has reduced the depth by 18% (now just 6.1mm) has had the effect of adding 3mm to the height due to rearranged internals. So old cases are generally a no-go if you wanted to upgrade from a mini 2 or 3. You really don't notice that extra length, but you do notice how thin it is – this is the chuck-in-a-bag iPad you've always wanted, and it feels less delicate than previous models. That's partly due to the air gap reduction in the screen – something the Air 2 rectified from the first Air. Elsewhere, the external changes are minor but there's no Mute/Lock switch; they are now virtual options in Control Centre.

The mini 4's new internals include the A8 and M8 processors found in the iPhone 6 and 6 Plus. The Air 2 had the A8X, so this mini is not exactly on par with its bigger sibling, which was evident in our tests. Using the GeekBench app, we clocked the mini 4 at an average of 3046 on the multi-core test, narrowly beating the iPhone 6 but still a bit behind the iPad Air 2's A8X. The inclusion of 2GB of RAM helps elevate the mini 4 beyond what the iPhone 6 and 6 Plus are capable of – but we're talking tiny performance gains in real life here. Essentially, this is just as powerful as the iPad Air 2 in real world use, and with iOS 9 it has superb all-round performance for managing documents, editing photos, and videos and games.

It's new features in iOS 9 which are exclusive to the top-end iPads that are the new mini's biggest draw. Split View is a wonderful new way to use your iPad, enabling you to have two apps open at once and usable at the same time. We still found it a nice addition , but the screen size is much reduced on an iPad mini, making it awkward at times to be truly productive with two apps. It's better suited to Mail and Calendar than Safari and Photos.

Previous minis have lacked the colour accuracy of the iPad Air 2 and recent iPhones. This is no longer the case; there's a clear gamut change here, offering much more vibrant colours. The mini 4 also has the same anti-reflective screen as the iPad Air 2, which helps in bright light situations. As for battery life, it easily matched Apple's quote of 10 hours of surfing the web or playing music or video.

Christian Hall

Verdict

Features	★★★★½
Performance	★★★★
Value	★★★★½

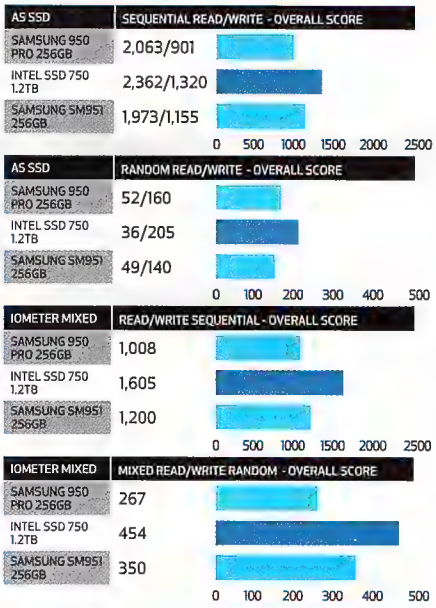
The iPad mini is back, and it's no longer the poor sibling of the 9.7-inch model. A good, if pricey, upgrade.

★★★★☆

$299 | WWW.SAMSUNG.COM/AU

LABS BENCHMARK RESULTS

Performance Category



Samsung 950 Pro 256GB

M.2 SSDs don't get the short end of the stick.

Never mind the small size; M.2 drives have the potential to deliver a ton of performance in a compact form factor. This makes them ideal for Ultrabooks and thin and light laptops, and desktop motherboards are getting in on the action as well. With SATA topping out at a theoretical 6Gbps, PCIe is the way forward, and M.2 leverages the PCIe bus to deliver up to 32Gbps. Add in support for NVMe (Non-Volatile Memory Express), an optimised protocol designed to let SSDs reach their full potential, and this looks like the way of the future.

So what's the problem? Until now, finding retail M.2 NVMe drives has been difficult and expensive. Samsung was the first to offer an M.2 PCIe SSD with its XP941, and it followed that with the SM951 earlier this year. Then it released the SM951 NVMe, a second iteration of the drive with NVMe support.

Unfortunately, these were designed as OEM-only products, going primarily to laptop vendors, where the OEM was responsible for ensuring the necessary features were in place. You could find those drives online, but without a warranty and at high prices.

The Samsung 950 Pro aims to change all that, with a five-year warranty plus some stellar performance for good measure. The change of heart likely stems from Intel's launch of Skylake and the Z170 chipset, which allows desktop M.2 to reach its potential. For optimal performance, you need a Z170 motherboard with an M.2 slot that supports x4 PCIe Gen3 lanes – anything less and you'll potentially hit a performance ceiling.

The 950 Pro is fast, but it can't beat the Intel SSD 750 in many of our benchmarks. Part of the reason is the smaller form factor of M.2, part of it is due to capacity, and some of it comes down to controllers and features.

The SSD 750 performs superbly, but it also takes up a PCIe slot and has a heatsink. In contrast, the 950 Pro is tiny and tucks away between PCIe slots on most motherboards. The 512GB 950 Pro also improves performance thanks to the increased parallelism the additional V-NAND chips offer. You might be surprised that even at a modest 256GB, Samsung wins out in the real-world file copy and PCMark 8 tests.

Both the earlier SM951 and the new 950 Pro have a feature called Dynamic Thermal Guard. In heavy workloads, it's possible for the NAND chips and controller to heat up and potentially malfunction, so the 950 Pro can throttle to avoid overheating. Samsung states that it does "not anticipate any performance drops due to thermal throttling," but we found that performance was up to 10 percent higher in random write tests when we had a fan blowing at the drive.

That's something to keep in mind. Samsung's 950 Pro may not win out in pure performance, but with better pricing and availability than the SM951, it's an easy win for anyone looking for an M.2 NVMe drive. It's a jump in pricing compared to SATA offerings, and it's clearly geared toward recent hardware platforms, but if you've got the funds and the necessary connector, it can make even the best SATA drive look sluggish. ■ **Jarred Walton**

Verdict

Features	★★★★½
Performance	★★★★½
Value	★★★★½

Great performance; good warranty; retail availability

★★★★½

THERMALTAKE
LIQUID COOLING

MADE FOR EXTREME PERFORMANCE

START YOUR LIQUID COOLED PC AT THERMALTAKE.COM

GERMAN MADE MATERIALS
ALUMINIUM ALLOY

BEST-IN-CLASS
COOLING PERFORMANCE

UNRIVALED COMPATIBILITY
& RELIABILITY

Tt®
Thermaltake

"Out of the box, the performance is pretty impressive, with the possible exception of its 4K read performance; however, the 4K write performance is strong in both RAID 0 and RAID 1."

NETWORK ATTACHED STORAGE

$459 | WWW.ASUSTOR.COM

Asustor AS5002T

Meaty two-bay NAS for home or office.

Asustor has a number of two-bay NAS units under various guises in its lineup. This model, the AS5002T, sits very near the top of the tree when it comes to both performance and feature set, and although it's aimed at the home/power user, it wouldn't be out of place in a small office.

It certainly doesn't lack for power, as at its heart lies an Intel 2.41GHz (2.58GHz Burst) dual-core Celeron J1800 backed by 1GB of DDR3L memory. There are two easily accessed SO-DIMM slots, allowing the memory to be expanded to 8GB if needed. Straight out of the box, the performance is pretty impressive, with the possible exception of its 4K read performance; however, the 4K write performance is strong in both RAID 0 and RAID 1.

The two drive trays support both 3.5-inch and 2.5-inch drives (including SSDs – ADM 2.4 onward supports the SSD Trim command), although you'll need a screwdriver to fix them in place. By using 2.4 and above versions of the ADM OS, drives up to 8TB are also supported, making for hefty storage options.

If you are used to looking at the rear panel of a NAS box and seeing nothing but an Ethernet port, and maybe a USB port, the rear of the AS5002T will certainly get your attention. It's loaded with ports to connect it with any other devices that might be available. There are two Ethernet ports, which support link aggregation for faster transfer speeds and better load balancing, and a couple of USB 3.0 ports – there's a third in the front bezel. The front one can be used for one-touch backups to an external drive. The rest of the ports comprise a pair each of USB 2.0 and eSATA ports, a single HDMI 1.4a output, and last but not least, an S/PDIF port. That's plenty of options.

Once the drives are installed, it takes very little time to set up the unit and load the ADM (Asustor Data Master) software. ADM (at the time of review, it was version 2.4.2) is one of the best GUIs out there, being both graphically rich and easy to navigate – that's good news, as there's a lot going on.

Need to hook up to the AS5002T on the move? Not a problem. Asustor's AiMaster is its NAS management app, which enables control of the NAS from a mobile device. The unit can be set up, managed, backups performed, files accessed, and even surveillance feeds monitored, all from your mobile device. The app also sends real-time event messages, should problems occur with the NAS.

Remember that HDMI port? Well, by connecting to a TV and using the Kodi 14.2 (aka XBMC) home theater software, the AS5002T turns into a media center, supporting up to 1080p output – quite the bonus. One nice feature is the ability to preview video files when browsing content with the ADM File Explorer.

As well as all those ports to use to back up data on an external device, the AS5002T also supports the Rsync (Remote Sync) function. This means data can be programmed to automatically back up to another Asustor NAS, or indeed any other Rsync supporting NAS on the network. And with over 100 apps in Asustor's App Central, covering pretty much everything from backups to web hosting, you can customize the AS5002T to your own needs.

■ Zak Storey

Verdict

Features	★★★★½
Performance	★★★★
Value	★★★½

Solid performance and a good feature set thanks to the ADM OS. The drive bays aren't tool-free, though.

★★★★½

MONITOR

$1,199 | WWW.ASUS.COM/AU

ASUS PG279Q

A genuine dream-screen for demanding PC gamers.

ASUS's latest entry into its Republic of Gamers (ROG) line is the much-anticipated PG279Q. This is the G-Sync version of the MG279Q that we reviewed last month – though it's got a few new tricks of its own, including the ability to run at a blistering 165Hz.

But let's start with the basics: 27-inch screen, tick. IPS panel, tick. 2,560x 1,440 WQHD resolution, tick. Add to this height, tilt, swivel and portrait support along with decently thin bezels and a solid stand. Finish with an easy to use OSD controlled by joystick and it's already winning over hearts and minds.

And how does it play? Gorgeous. The IPS panel gives rich colours and superb contrast, which along with the WQHD resolution is a dream to game on. If you're used to TN-based panels, you won't want to go back. Utilising G-Sync will prevent tearing and provide a more stable image if you fall below your chosen refresh rate – typically 60, 120, 144 or 165Hz. And thanks to a 'Turbo' button on the monitor, you can change between these modes without exiting your game.

Two other modes are supported: ULMB (Ultra Low Motion Blur) and Fixed Refresh. ULMB and G-Sync are mutually exclusive, so this depends on what you prefer. If your rig can push the maximum refresh you're after (say 120Hz), G-Sync is less important and ULMB will give you a better image with reduced motion blur.

A bevy of other features are included too such as 'GameVisual' modes that encompass Scenery, Racing, Cinema, RTS/RPG, FPS and sRGB. These are okay, but generally you'll have more success manually tweaking parameters to your liking. And the 'Game Plus' bundle throws in a centred crosshair, timer and FPS counter, the latter being the most useful as it allows you to see FPS without using any monitoring software.

One great addition are the blue-light filter modes. This actually makes a big difference to reduce eye strain, especially if you're playing or working late at night, but you will lose accuracy of colours at the higher levels.

Unlike other G-Sync displays the PG279Q includes more than just a DisplayPort connector. Here there's an additional HDMI port, but this is a little confusing as it's HDMI 1.4 and can only drive the display at 60Hz – ergo, buy this for the high refresh rates if you have DisplayPort.

There's another restriction to be aware of, too: in order to use the 165Hz 'overclock' mode, an Nvidia 960 or better GPU is required. According to ASUS this isn't about driving the display at that speed, but a function of how the latest G-Sync module in the PG279Q interacts with the GPU to support it. On other Nvidia cards you'll be limited to 144Hz (if you call that a limit!).

Which raises the question, how effective is 165Hz? It's hard to spot the difference between 144Hz and 165Hz, despite the fact it's almost as large a jump as from 120Hz to 144Hz, which you can more easily discern. There is still room for our eyes to pick up subtle differences in smoothness as refresh rates increase, but we're clearly getting close to what most people will be able to notice.

The only thing not to like here is the price – at $1,199 you could get a decent 30- or 34-inch monitor. Thank the G-Sync premium for that, which requires an add-on module. ■ **Ashton Mills**

Verdict

Features	★★★★½
Performance	★★★★★
Value	★★★½

The PG279Q ticks every box and then some. G-Sync adds a premium, but if money is no object, this is unmatched.

★★★★★

apc RECOMMENDS

BUSINESS PRINTER

$699 | WWW.EPSON.COM.AU

Epson Workforce ET-4550

More ink than you'll probably ever need.

Small office inkjet printers usually stand out from each other based on print speed and quality. Not so here. Instead, this unit has a unique value proposition. And that is tons and tons of cheap ink.

Compared to similar Epson all-in-ones, this new EcoTank model (one of five in the range) is capable of storing the equivalent of up to 20 previous-generation ink cartridges. That equates to at least two years of ink, or 11,000 black pages or 8,500 colour pages.

The ET-4550 is a workhorse printer that produces moderately fast prints with little to no image complexity or colour accuracy. But at least it will print and print and print without you always having to think about when to replace the ink.

The ET-4550's body is a fingerprint-proof, matte black plastic. You'll find several compartments, including an upper tray, a scanning bed that holds up to an 21.6 x 35.5cm sheet, a collapsible front-facing output tray that holds up to 150 A4 pages, and a tray which can hold up to 20 envelopes and other small form-factor pages.

On the far right-hand side of the unit is the bulky compartment where the ink is held. On a typical printer, your ink cartridges are housed within the body of the unit. With the ET-4550 Epson chose function over form by adding a three-inch-wide, four-compartment container to the right-hand side of the unit, into which black, cyan, magenta and yellow ink bottles are poured. The compartment gives the unit an unorthodox look and feel – the jutting ink containers are an eyesore. Bad looks aside, it comes with four bottles of ink, three colour bottles (roughly 100ml each) and one massive (200ml) bottle of black ink. Epson claims this is enough to keep you printing for more than two years. A new set of bottles will cost $76.

However, be careful when emptying the bottles into the compartments. They leak and spill easily. Epson provides you with gloves for this dirty work, and you'll need them. Once your printer is full of ink, getting the ET-4450 to work is fairly straightforward, but it is a lengthy process, as it needs a 20-minute ink calibration.

The ET-4550 measures 250 x 35 x 24cm and is just 7.2kg. As for performance, manufacturer-provided specs can be quite deceiving. Despite claiming print speeds of 13 black pages per minute and five colour pages per minute, we were only able to print five Word documents in black and white in 60 seconds. It failed to print even one colour image in under a minute, and took two minutes to produce a colour photo on plain paper.

These speeds are pretty slack, especially for a workforce printer. You can accept 13 black images per minute if the image quality was top-notch, like the Canon Pixma MG7520. But with a top resolution of 4,800 x 1,200 dpi, the ET-4550 needs to be much, much faster than it is.

The prints don't come out badly, though. The blacks are bold and the bright colours pop. However, there isn't much contrast here; your darks fade into one another and the detail output isn't complex. If you need a printer for company memos and homework assignments, then this is all you really need. But if you're trying to print vibrant photos or if you need to run off a ton of copies quickly, look elsewhere.

Verdict

Features	★★★★½
Performance	★★★☆☆
Value	★★★★★

If your main concern is keeping costs down, this might be the ideal printer for you.

★★★★½

LABS RESULTS: GRAPHICS CARDS

GENERAL PERFORMANCE	MSI GTX 950 GAMING	ASUS STRIX-GTX950-DC2OC-2GD5-GAMING	GIGABYTE GV-N950XTREME-2GD
PEAK TEMPERATURE	70	68	69
GAMING PERFORMANCE (LOW/AVG FPS)	**MSI GTX 950 GAMING**	**ASUS STRIX-GTX950-DC2OC-2GD5-GAMING**	**GIGABYTE GV-N950XTREME-2GD**
BATTLEFIELD 4	27/54	28/54	28/55
TOTAL WAR: ATTILA	10/21	10/21	9/24
GRID 2	64/81	63/81	65/83
GTA V	11/37	11/35	12/37
SHADOW OF MORDOR	14/33	15/36	15/36

All tests carried out at 1080p with average details.

GRAPHICS CARD

$269 | WWW.ASUS.COM/AU

ASUS STRIX-GTX950-DC2OC-2GD5-GAMING

Is factory overclocking worth it?

With a bit of a gap in the budget GPU line-up that was only getting filled by AMD, Nvidia has recently released the GeForce GTX 950 to compete. It was a solid move; it's faster than AMD's Radeon R7 370 and almost as cheap.

The 950 is built around the same GM206 core as the GTX 960, just scaled back a little. It has six instead of eight SSM units (and thus 768 instead of 1,024 CUDA cores), but the same 32 ROPs and 128-bit memory bus.

While no-frills versions of the 950 exist, ASUS has slapped a STRIX stamp on this model, meaning it's a cranked-up version designed for mainstream gaming. That means it gets bonus features like ASUS's DirectCU II+ heatsink, which lets it run cooler and gives extra overclocking capacity. Backed up with 2GB of RAM, the 1,188 MHz default boost CPU clock has been pushed up to 1,355 MHz here, while the base clock is 1,165 MHz instead of 1,024 MHz.

The result is a card that performs faster than a stock model, yet doesn't sound like a small plane taking off. For less-intensive games like League of Legends, this also means the 950 GPU can actually leave the fans off and run completely silently. As with others of its kind, this 950 has dual DVI, HDMI and DisplayPort outputs.

The STRIX will cost you 10% more than cheaper stock 950s, but in benchmarks it offers only a little extra performance. What that $25 is buying is a much cooler-running card that still has some extra OC potential – and you can use it with ASUS's excellent software too.

Lindsay Handmer

Verdict

Almost worth the extra cost over stock, but faces stiff price competition from the GTX 960.

GRAPHICS CARD

$285 | WWW.GIGABYTE.COM.AU

Gigabyte GV-N950XTREME-2GD

Is this the fastest GeForce GTX 950 you can find?

At launch, Nvidia's budget-oriented GeForce GTX 950 had one main problem: it was hard to find for a price much lower than the GTX 960 – a more powerful card that gives you around 10% extra performance. But prices have started to settle down, and the GTX 950 can often be had for around 10% less than its faster sibling. However, the GPU buying waters get muddied once you start considering the overclocked 950s with aftermarket heatsinks that are now available.

The Gigabyte Xtreme Gaming is one of the latter, and it pushes the speed further than any other 950 we've tested, with an overclocked core than can boost to 1,405MHz. That's enough for an extra few frames a second, which can help at this lower end of the spectrum. It also pushes its 2GB of GDDR5 RAM up to 7,000MHz.

The extra performance is made possible thanks to the custom cooling system, which uses direct-contact copper heatpipes and twin fans. Under low load gaming conditions, the card can even run silently. The GPU also features DVI, HDMI and three DisplayPort outputs, plus some funky LEDs. Additionally, you get higher-end components such as capacitors, plus the OC Guru II software.

This Gigabyte card offers excellent performance and a high-quality build, but it's let down by its price. Its biggest competition is the GTX 960 – an overclocked Gigabyte model is the same price as this Xtreme Gaming unit, and despite having a lower core clock speed, the 960 still offers better overall performance.

Lindsay Handmer

Verdict

A very compelling budget card, except for the still too-high price.

PORTABLE KEYBOARD

$99.95 | WWW.ZAGG.COM

Zagg Pocket Keyboard

Zig-zagging towards a compact smartphone keyboard.

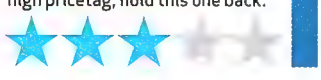
Measuring over 22cm long, Zagg seems to have been a little optimistic in calling this a pocket keyboard – unless of course you've got pockets deeper than Bill Gates. That said, it's comprised of four distinct panels that allow the device to concertina into a single compact slice, and fold-up into the most portable smartphone keyboard we've seen.

Two of the four panels are dedicated to the keyboard, while the remaining two make a right-angled A-frame stand which can hold a smartphone or tablet. While this design is certainly interesting, there are no braces built into the stand, so its plastic hinges sag under force and make the keyboard feel flimsy. This problem continues into the keyboard, which can be overextended if not flat on the table and further contributes to a somewhat 'economical' overall feel – a little problematic considering it's actually $25 more expensive than some excellent alternatives.

The Zagg Pocket Keyboard manages to avoid swapping from a traditional key layout and thankfully doesn't remove any integral buttons. Battery life and connectivity were both solid, though swapping between Android and iOS connections was a little fiddly. All things considered, the Zagg Pocket keyboard is pretty good – the only thing we missed were dedicated play/pause and unlock shortcut buttons – but the flimsy design and premium price tag make it a little hard to recommend over the competition. ■ Joel Burgess

Verdict

Design and build-quality shortcomings, combined with a high pricetag, hold this one back.



PORTABLE KEYBOARD

$129.95 | MICROSOFTSTORE.COM

Microsoft Universal Foldable Keyboard

Clamshell contender.

We were pretty happy with Microsoft's Universal Mobile Keyboard when we tested it in the *APC* labs a few months ago. So when we heard that the company was bringing out an additional smartphone keyboard, we were curious to see why Microsoft would take another crack at something it'd arguably already nailed.

Open up the Universal Foldable Keyboard and you'll see it takes up about the same space as your average laptop keyboard but the keys are split into two distinct halves to allow the keypad to fold. To accommodate that gap, the keys are fractionally smaller and have no space between them, undoing any benefits associated with the larger surface area. Though touch typing is initially awkward, it's partially rectified by an oddly shaped key structure that sees supersized 'T' 'G' 'H' and 'N' keys.

Microsoft has kept some of our favourite features of the Universal Mobile Keyboard; the volume controls, a lock/unlock button and a toggle for the three smartphone platforms. Two new preset buttons can connect two separate devices and flick between them.

Unfortunately, there's one major thing missing: a stand for your smartphone or tablet, and it's something that can seriously improve the typing experience. Then there's the price. You can pick up the older Universal Mobile Keyboard for $75, whereas this new model costs $130. Despite excellent features, asking almost double the price doesn't quite justify the new additions. ■ Joel Burgess

Verdict

A solid smartphone keyboard, but the high price counteracts the new benefits.

$369 | WWW.MOTOROLA.COM.AU

Motorola Moto G (2015)

G is for great.

The third generation Moto G is proof that you don't need to drop a ton of money to get a decent phone. It doesn't have the fastest processor, the sharpest display or the best camera, but it does punch above its weight class in all areas.

Importantly, it offers IPX7 waterproofing, which means it can withstand immersion for half an hour at a maximum depth of one metre – more than enough for casual water activity and accidental spills. The all-black plastic enclosure isn't much to look at, but you can brighten up its drab appearance with optional coloured backplates.

Sadly, the excellent Moto Maker service available in other countries, which enables you to customise the design of certain Motorola devices, isn't available in Australia, although local reps have promised it will arrive sometime next year.

The Moto G's performance matches devices that cost twice as much. This is partly thanks to the speedy quad-core 1.4GHz processor and 2GB of RAM, and its use of a nearly stock Android 5.1.1 operating system. Motorola has added a few light enhancements that don't drag the system down (which is more than we can say for Samsung and HTC) and actually add value, such as the enhanced Moto Display lockscreen notifications and Moto Assist's smart contextual learning engine.

While most device manufacturers steer towards larger displays and non-expandable storage, the Moto G is a nice counterpoint, with a compact 5-inch 720p display and microSD expansion to augment the built-in 16GB of storage. ■ Jenneth Orantia

Verdict

A great midrange all-rounder at a very keen price.

★★★★½

PAYAM Data Recovery

AUSTRALIA'S #1 DATA RECOVERY COMPANY

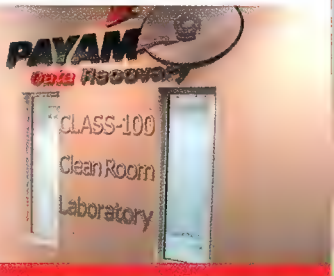
OFFICIAL WESTERN DIGITAL DATA RECOVERY PARTNER IN AUSTRALIA AND NEW ZEALAND

THE ONLY AUTHORISED SEAGATE DATA RECOVERY SERVICE PROVIDER IN AUSTRALIA AND NEW ZEALAND

EXPERT DATA RECOVERY FROM
Damaged Hard Disk Drives, SSD, RAID, NAS, Mobile Phones, USB Flash Drives and Memory Cards.

Are you an IT Professional?
Join our Free Partnership Program today.
www.payam.com.au

See our CLASS-100 CLEAN ROOM at www.payam.com.au



Data Rerovery Labs in Sydney, Melbourne, Brisbane, Perth, Adelaide and Auckland (New Zealand)

1300 328 273 help@payam.com.au

www.payam.com.au

FROM $1,099 (32GB) | WWW.SAMSUNG.COM/AU

Samsung Galaxy Note 5

A notable successor, despite a few character flaws.

It's no huge secret that Samsung's been struggling when it comes to smartphone sales this past year. A saturated market combined with Apple's launch of bigger iPhones have hurt the Korean giant, which has outright stated that it hasn't sold as many Galaxy S6 phones as it would have liked.

But in Samsung's defence, its current phones are the best its ever made – the glass-and-metal materials make for enticing, well-wearing phones that feel like premium devices, the performance and battery life are class-leading, the AMOLED screens are miles ahead of any LCD and even TouchWiz, Samsung's historically lackadaisical Android skin, is more polished, professional-looking and faster than ever. The Korean company seems to have finally eliminated the problems that made its phones feel sluggish compared to other premium Android vendors.

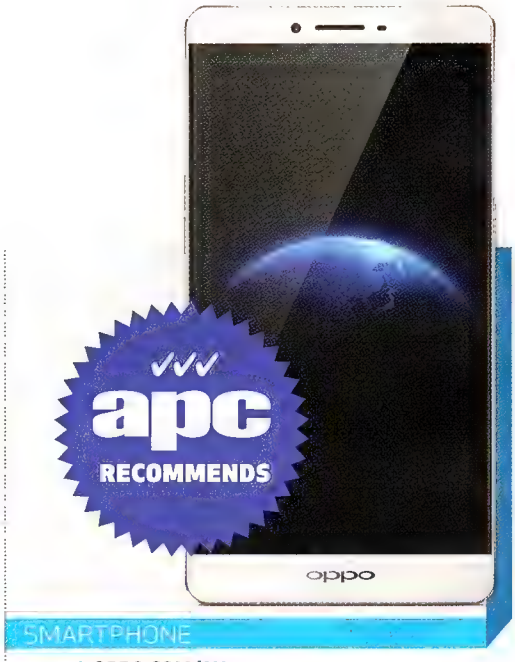
The Note 5 benefits from all that, and Samsung's somehow slimmed it down even further from last year's model, and with the fingerprint sensor now a fast optical model, the phone's much easier to hold and use one-handed.

In fact, this is pretty close to being the perfect big-screen phone, with class-leading performance. We do have a handful of gripes, though. It only comes in 32GB and 64GB options, while the glass front and back means it can also be a bit slippery in the hand. For many, those shortcomings will be easy to overlook. The Note 5 finally manages to cram a 5.7-inch screen into a body that feels and looks truly elegant.

Dan Gardiner

Verdict

A great display, first-rate build and top performance make this the best plus-sized phone around.



$599 | OPPO.COM/AU

Oppo R7 Plus

Breaking the glass ceiling of the mid-range smartphone.

Though the 6-inch Oppo R7 Plus maintains the appealing shape and look of its smaller R7 sibling, there are quite a few features that make this bigger model a unique proposition that stands out in its own way.

The most noticeable is the movement of the Home, Back and Menu buttons; on the R7 they're physical and placed below the screen, while the Plus has software based ones, contained on its touchscreen. But the most significant upgrade is the addition of a rear-mounted fingerprint sensor, which sits underneath the rear camera. Oppo's latest Colour OS, which is essentially a tweaked version of Android 5.1, looks great on the 1080p AMOLED display, while the impressively thin bezels and polished metal case combine to give the phone a largely premium feel. And though you might expect this from your smartphone, it's not always the case for mid-level phones that go for $599 – especially not phablets with 6-inch displays.

Performance wise, the R7 Plus is closer to where you'd expect from that price; it manages respectable benchmark scores for general tasks, but only just scrapes in when it comes to more intensive gaming tests. The Plus's Qualcomm Snapdragon 615 processor has two A53 quad-core ARM Cortex chips, one that runs at 1.7GHz and the other at 1.0GHz, to maximise efficiency without having to sacrifice performance in more demanding tasks. In combination with the Plus's huge 4100mAh Li-Po battery, this big phone still gets a 10.5-hour battery life and even allows close to 6 hours of continuous gaming.

Joel Burgess

Verdict

Solid value for the asking price, though the performance and overall build quality do match that RRP.

SUBSCRIBE TO APC AND GET 6 ISSUES FOR $45!

12 ISSUES FOR ONLY $69

WHY SUBSCRIBE?

- Take advantage of our trial subscription offer of six issues for $45 if you choose to auto-renew*
- Or get 12 issues of Australia's favourite tech mag for only $69!
- Save even more, with 24 issues for $128. That's only $5.30 per issue!
- Free delivery of every issue straight to your door
- Free disc with exclusive software in every issue**

SAVE UP TO $110!

WIN! LG 34in MONITOR
SEE PAGE 15!
apc
BUILD A COMPLETE SECURITY SUITE FOR FREE!
THE NO-BS PLAIN ENGLISH GUIDE!
MAKE A FAIL-SAFE WINDOWS BACKUP
DON'T GET CAUGHT OUT-FOLLOW OUR STEP-BY-STEP BACKUP PLAN
DIGITAL PRIVACY & SECURITY
REVEALED: WHAT THE REAL THREATS ARE + HOW TO PROTECT YOURSELF ON ALL YOUR DEVICES
HOTTEST TECH REVIEWED
ASUS's ultimate gaming monitor
Pocket keyboards
The amazing printer with 2-year ink tanks
Apple iPad mini 4
SECURITY APPS & SERVICES
VPN subscriptions: who's got your back?
Password managers: safe and easy to use
Android security apps: why you need one
RASPBERRY PI MEDIA PC
In-depth tutorial: Build & customise a powerful, flexible & low-cost media player
Future

FREE DELIVERY TO YOUR HOME OR OFFICE EACH MONTH

HURRY

OFFER ENDS DEC 9TH, 2015!

TWO EASY WAYS TO SUBSCRIBE TO *APC* MAGAZINE

VISIT www.magshop.com.au/future

OR

CALL 13 61 16 and quote M1512APC

TERMS & CONDITIONS This offer expires December 9th, 2015, and is available to subscribers within Australia only. Please allow 6-8 weeks for delivery of your first issue. For full terms and conditions, see www.magshop.com.au/future. Please see our privacy policy on page 3. *Six issues for $45, then $45 charged to your credit or debit card every six issues thereafter on auto-renewal. **Disc only included with AU copies, NZ content is downloadable.

software

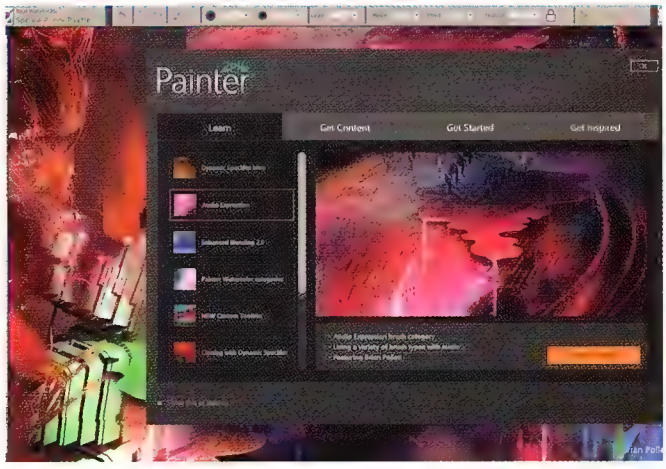
» APPS FOR ALL THE PLATFORMS

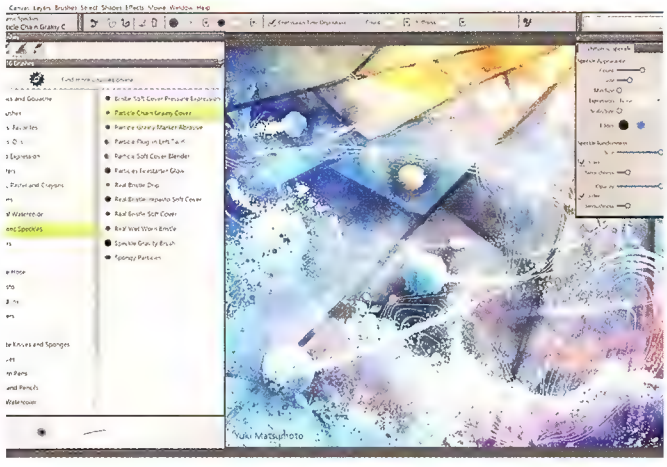
Windows SOFTWARE

Corel Painter 2016

Add some new tools to your digital paintbrush and easel.

$429 | WWW.PAINTERARTIST.COM/AU

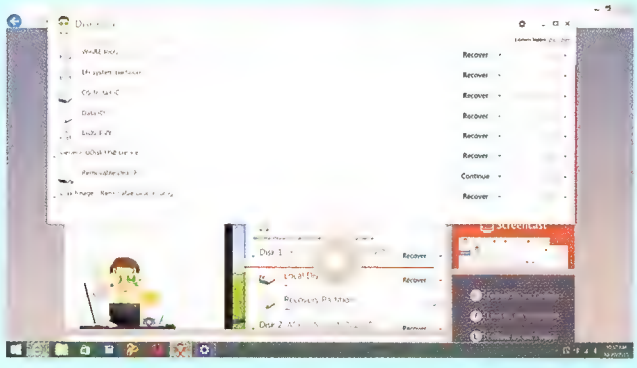




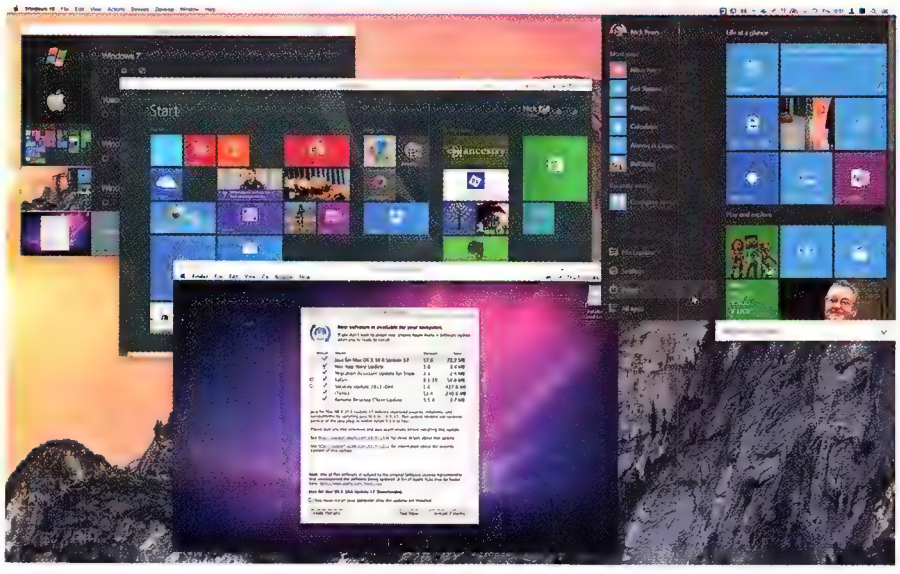
As soon as you launch Painter 2016 you're shown a redesigned welcome screen that gives you access to helpful tutorial videos. This is a great way to discover more about Painter's new features, even if you've used an older version. As before, the 2016 edition has an abundance of brushes and effects including a number of new and more unusual effects, such as the rather fun Dynamic Speckles. Though we found a lot of the brushes in this set to be fairly ordinary, the Particle Firestarter Glow gave a nice random 'firework'-type effect, and the Audio Expression brush sees your brushes' size, colour and other attributes changing in time to music, allowing for some interesting and unique results. It makes for a fun addition to your toolset, although we doubt it will get much use after the novelty has worn off. Painter is by far the best digital easel out there, and this new version maintains that status. With plenty of tools and functionality packed in, we certainly think that it's well worth the money if you're after a great app for creating digital art. That said, if you already have Painter 2015, the new features probably aren't worth the money – even at the lower $229 upgrade price. Yes, the new tools are fun, but it's unlikely they'll become a key part of your toolset. **James Robinson**

Disk Drill

FREE | PC.CLEVERFILES.COM



Disk Drill is a data-recovery application for Windows and Mac that can dig into your hard disk or flash drive and uncover deleted or corrupted files. Working with both external and internal drives, when run it'll throw up a list of all the locations you might want to recover lost or corrupted files from — just select one and it scans the drive using a number of different algorithms to detect any bits of information on the drive that are still in a readable format. Disk Drill can recover deleted files in FAT, exFAT or NTFS filesystems. The interface is simple and effective allowing you to select a recovery destination folder and even save session progress to resume it later — useful if you're planning on recovering an entire hard drive. Though most files will be revealed with one of the software's quicker scans, you also have the option to go through the entire drive bit by bit using the deep scan option. In addition to recovering files, Disk Drill can also scan for lost partitions and can keep a log of everything you delete from your computer, in case you need to find it again later. It can also be used to do a full disk image backup which can then be transferred to another device or reinstalled to the original disk. Disk Drill is pretty great for a free application, especially when you consider it doesn't even have any ads. **Joel Burgess**



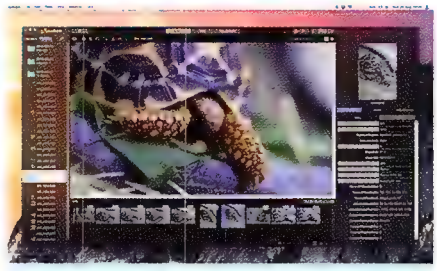
Parallels Desktop 11 for Mac

A fast and effective way to run Windows and other operating sytems inside OS X.

FROM $99.99 | PARALLELS.COM

Parallels Desktop allows you to run alternative OSs within OS X. It's far more flexible than free rival VirtualBox, and version 11 continues to improve performance while adding handy new features. A key reason to get it is El Capitan and Windows 10 support – the latter runs in Parallels 10, but it's not officially supported or optimised. Parallels 11 sweetens the deal by using its standout Coherence mode to integrate key Windows 10 apps and features directly into your OS X desktop, most notably the new Notification Centre, which closely resembles OS X's own, and the Cortana search assistant (though the latter isn't available in Australia yet). Parallels 11 also makes one of OS X's underrated features available to your virtual machines. Quick Look isn't available in Windows, but with Parallels you can press the spacebar within your VM to preview a file in OS X. On a MacBook, Travel Mode promises to cut power consumption by VMs to prevent them quickly draining your battery. It's enabled in each VM's settings. As with previous releases, Parallels 11 promises improved performance. The best improvements are in processor usage, particularly when using multiple cores, but aside from when booting a Windows 10 VM it's not obvious. Still, the gap between virtual and native performance gets that bit narrower – with one notable exception: Parallels 11 is stuck using DirectX 10 technology, which means graphics performance is no better than in Parallels 10. Ultimately this translates to one key thing: hard-core gamers are better off using Boot Camp, but for everyone else, Parallels makes everyday computing a breeze, so long as you have the CPU, RAM and drive space to spare. The new subscription-based Pro edition has a consequence for regular users. Each VM is now limited to four processor cores and 8GB RAM. This won't affect most people, but power users should take note.

Nick Peers



Emulsion

US $50 | EMULSIONAPP.COM

An app called Emulsion sounds like it's going to be a collection of film-effect filters designed for people with interesting facial hair, but in reality this is a Lightroom-a-like that can organize and non-destructively edit your photos.

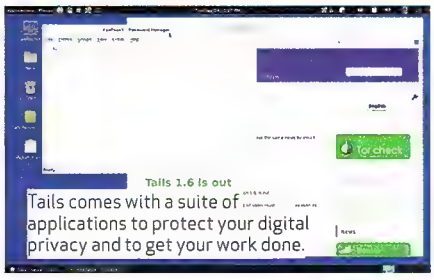
Getting your images into the app couldn't be simpler. Once a folder has been added to Emulsion, the program monitors it for changes, so if you add new photos you won't have to freshly import them.

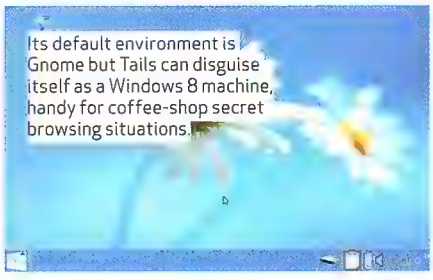
For metadata addicts, Emulsion has it all. The searchable EXIF covers not just camera model, focal length and shooting parameters, but camera temperature, firmware version and whether you used Live View or not. A lot of the basic data is editable, and you can build a list of your equipment to easily populate the EXIF of scanned film images. A tool palette lets you crop, rotate and clone out spots, then a click across to the Adjustments palette on the right enables image editing, although not until you've created a Version.

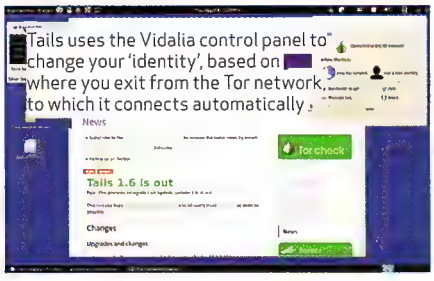
Sensibly, Emulsion restricts editing to a copy of your image in order to preserve your master, although this surely could have been achieved in the background without prompting you to enter a name every time. There's an auto-enhance option accessible from the cog icon, while the sliders icon next to it brings out a palette of one-shot filters. Any adjustment can be unchecked to remove it from the image.

The downside of the app is that it's a bit slow, with plenty of pauses between adjusting a slider and the effect appearing. It taxes the CPU too, kicking our MacBook's fans into life when processing raw files.

Ian Evenden




Its default environment is Gnome but Tails can disguise itself as a Windows 8 machine, handy for coffee-shop secret browsing situations.


Tails uses the Vidalia control panel to change your 'identity', based on where you exit from the Tor network, to which it connects automatically.
Tails 1.6 is out

Tails 1.6

Les Pounder pretends to be a secret agent with this privacy-focused Linux distro.

FREE (OPEN SOURCE) | TAILS.BOUM.ORG

Protecting your online identity is not something that everyone has to consider, but for some – journalists or activists, for example – the need to anonymise their identity can be a matter of life and death. Tails (The Amnesiac Incognito Live System) is a Debian-based Linux distro that provides a secure connection to the internet and aims to preserve your privacy. Tails is available as an ISO image and can be written to USB or an SD card, or to DVD as a tamper-proof platform.

When booting Tails you can access an Advanced menu with options to create an administrator password (useful for further configuration), and also spoof your device's MAC address to avoid it being used to uniquely identify you. You can disguise Tails with a Windows 8 desktop environment so that you can blend in while working in a coffee shop. By default, though, Tails 1.6 uses the Gnome desktop environment and comes with the default Gnome applications, such as the Nautilus file manager and NetworkManager.

SECURE CONNECTION

The main feature of Tails 1.6 is that it automatically handles your connection to the Tor network via Ethernet or Wi-Fi. This is a great feature that has previously required manual configuration. Tails uses the Tor Browser, a secure version of Mozilla's Firefox, which comes with Tor Button, HTTPS Everywhere, NoScript and AdBlock Plus extensions. The browser won't run any JavaScript, Java, Flash or other background applications which may leak data. In fact, the browser's so secure that it wouldn't let us upload screenshots to Flickr by disabling access to the underlying file system.

But Tails is not just Tor for dummies, it's a full distro with a suite of tools. On top of the typical applications found in many distros it includes MAT (Metadata Anonymisation Toolkit), which is used to scan files for information that can be used to identify or trace a file to an individual. There's also the Electrum Bitcoin Wallet, used to keep your crypto currency safe with a layer of encryption – to use it you need to install Tails or create a persistent volume to contain your wallet. Traverso is a multi-track audio recording application. Gobby is a collaborative editor, mainly used by remote teams who wish to work on a project together. GtkHash generates a unique hash for a file, enabling the hash along with the file to be transmitted to a recipient and used to identify if any tampering has occurred in transit.

For those times where you really need an 'unsafe' browser, Tails comes with such an application, but it will remind you that your actions are not anonymous or secure. Applications all feature AppArmor, which reduces the risk of them being exploited or hacked. Hidden in the terminal is the popular aircrack-ng application used to audit the security of a network by trying to break the keys that protect it.

On our test machine, with an Intel quad-core 2.4GHz CPU and 4GB RAM, the desktop was responsive and there was very little lag, even when run from a USB flash drive. Lag can be reduced further by installing Tails onto a fast SD card. Tails can be run on a machine with 1GB of RAM, which makes it ideal to use with an old netbook when travelling and using public Wi-Fi, which may try to inspect your data.

A handy feature of Tails is that it can wipe information from RAM, which in normal use can retain information that can be recovered by an expert.

TALKING ABOUT TOR

You might be thinking that Tails is an ideal distro for file sharing, but although you can route your torrents via the Tor network this kind of activity is frowned upon as you are consuming vast amounts of bandwidth that has been donated to serve the needs of others.

Tor isn't an all-encompassing solution for digital anonymity, either. In fact, no one service can fully protect you, and there have been reports of authorities compromising exit nodes and locating users via their browsing habits. For true protection, you need to use a mixture of multiple services and change your habits.

Tails 1.6 sees a few changes from the previous major release, mainly upgrades to the Tor Browser, which is now based on Firefox version 38. The anonymous overlay network used by applications to send information securely, I2P (Invisible Internet Project), has been updated. There are updates and bug fixes to the SSL certificates and bind9, used for DNS services.

I've previously tested a few privacy-focused Linux distros, and when I last performed a broader comparison, Tails (at version 1.3.8) finished in second place just behind JonDo Live-DVD. With the release of Tails 1.6, that decision still stands. Yes, Tor is faster than JonDo when it comes to network connectivity and Tor is better when randomising node selections, but in essence Tails is still pretty much Tails in this latest version.

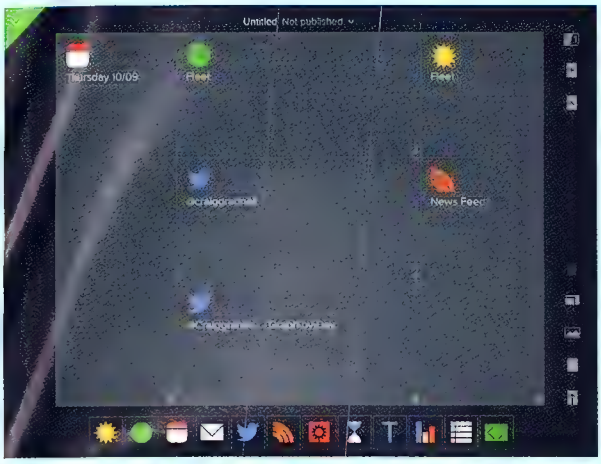
What it's good at is offering a very simple entry to keeping anonymous online, and it comes with a fairly comprehensive suite of applications for many day-to-day tasks. It's a good choice for its intended purpose, to help information be free.

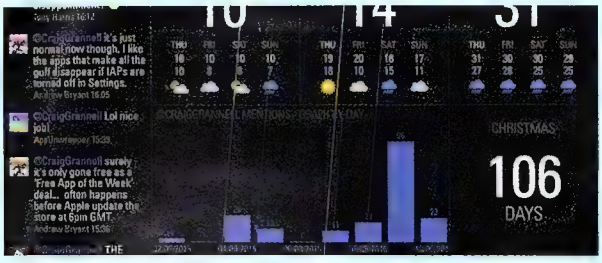
Guerilla Filmmaker

Unlock your inner Kubrick with your iPhone.

$4.99 | GFM-APP.COM

The best camera, they say, is the one you have in your hand. With this in mind Sotcha has created the Guerrilla Filmmaker app, which unlocks manual options for the otherwise automatic features of your iPhone's video mode – such as focus – but that's actually just the beginning. It's the programmable keyframe feature that makes this app so useful. All the manual features can be programmed to change their values at pre-designated intervals. That means if you have a tracking shot and want to pull focus between two focal planes you can program your focus shift, hit record and let the app worry about hitting the marks. For filmmakers, this is a truly amazing feature and one that few pro cameras have. The interface is likewise well designed and intuitive. That said, it's not perfect. There's no manual aperture control so depth of field is locked; and a more 'real-world' interface would have possibly helped camera pros pick it up and use it more rapidly. Still, Guerrilla Filmmaker represents superb value for money and has real potential for smartphone-loving indie filmmakers. **Alun Pughe**

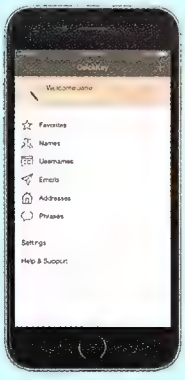




Status Board

FREE WITH IAP | PANIC.COM/STATUSBOARD

Status Board enables you to arrange a number of customisable panels which turn your iPad into a display that details all kinds of information. For free, you get panels for clocks, weather, calendars, email, Twitter and RSS feeds. Pay $9.99 and you can add tables, DIY HTML, graphs, countdowns and custom text. Smartly, photo albums are part of the paid offering, which we suspect will tempt many to upgrade. The panels look great, although be wary of the built-in wallpapers, which too often obscure on-screen text; and while we found some aspects of editing a touch fussy, it's easy enough to get everything up and running. For businesses, it's potentially an even better install. Boards can be shared as set-ups or stills, and you can enable subscriptions, so everyone's always got the latest version. **Craig Grannell**



QuickKey

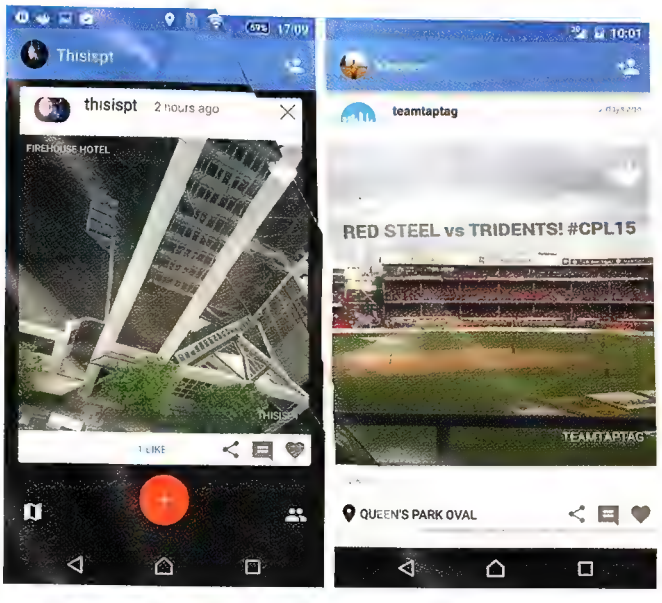
$5.99 | QUICKKEY-APP.COM

QuickKey is an iOS keyboard that replaces letters and numbers with pre-defined snippets. The app component enables you to define names, usernames, emails, addresses and favourites. These are then accessed in the keyboard by tapping the relevant icon and then the snippet itself. Setup is straightforward, and you can import individual contact info to speed things along. Lists are always presented in alphabetical order, which is awkward if you have many; an exception is the favourites list, in which items can be manually reordered. In use, it's fine, but nothing more. The app has potential to speed things along, but it awkwardly abbreviates addresses, has a delete key that ignores long-press, and comes with the associated general baggage of iOS third-party keyboards (that is, the overall system being quite clunky and unwieldy). It's useful, but by no means essential. **Craig Grannell**

Tap Tag

Crowd-powered app aims to build a visually-oriented travel guide.

FREE | TAPTAGIT.COM

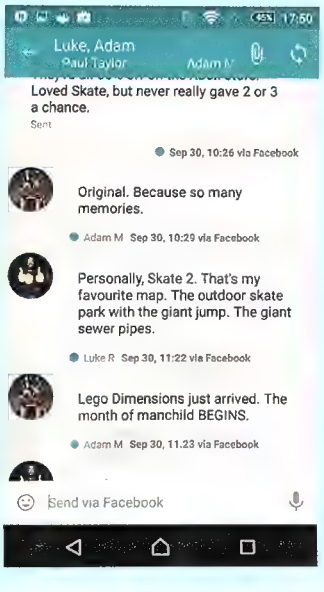


Tap Tag can be easily described as a cross between Twitter, Tumblr and FourSquare, a social media tool that has a slight uphill battle since all three of the aforementioned services are so pervasive. Tap Tag's both a tool to help you discover something new and unique in your area, and to share photos of what you've discovered — what happens from there is only limited by your creativity and urge to inspire others. Take a photo and the location's automatically added. Then, you stick a caption on it, and wait for the followers to roll in. Right now, it's early days for Tap Tag here in Australia — it's slowly ramping up on the west coast of the US — so the majority of posts are a bit, well, dull. It really needs a search function and more customisation options, but there's plenty of potential for it to be a platform for finding new places and telling stories. **Paul Taylor**

Disa

FREE | WWW.DISA.IM

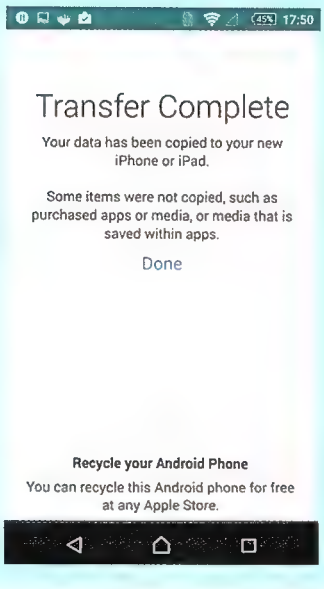
There's little joy in a connected world and fast, free messaging services when you spend a good chunk of your time trying to keep track of your texts, remembering who said what and on which app. Disa's aim is to act as the conduit, helping you keep track of all your conversations, no matter whether they're from SMS, Facebook Messenger, WhatsApp, or more. Right now, Disa only ties together the last three, but it encourages you to write your own plug-ins so you can have conversations flowing across Skype, Twitter and more — or more realistically, you can sit back and wait for someone else to invent these plugins for you. Despite the pleasant interface, there's a definite Wild West feel to Disa, as support relies on the common people: anyone who's security conscious (and that should be all of us) will need to pay close attention to what info the third-party plug-ins use and track, though Disa itself is very transparent. With more support and plug-ins, this could be a winner. **Paul Taylor**


Luke, Adam
Paul Taylor
Loved Skate, but never really gave 2 or 3 a chance.
Sent
Sep 30, 10:26 via Facebook
Original. Because so many memories.
Adam M Sep 30, 10:29 via Facebook
Personally, Skate 2. That's my favourite map. The outdoor skate park with the giant jump. The giant sewer pipes.
Luke R Sep 30, 11:22 via Facebook
Lego Dimensions just arrived. The month of manchild BEGINS.
Adam M Sep 30, 11.23 via Facebook
Send via Facebook

Move to iOS

FREE | TINYURL.COM/APC422-MOVE

So, you've decided to swap platforms from Android to iOS and are looking for the easiest way to transfer everything to your new iPhone? You've found it — sort of. While this app does a fine job of holding your hand all the way through the process (which should be less than the amount of time it takes to make and then consume a cup of tea), it will throw a slew of confirmation text boxes your way, asking you to re-enter your passwords on your old and new devices, over and over. That annoyance aside, it's simple to get started: join the same Wi-Fi network on both phones, start the app, and you're on your way, porting photos, text messages, and accounts. But, if you have everything synced to the cloud, the only really useful function of the app is copying text messages. And, you still have to redownload all of your apps — well, those that are available on iOS anyway. Still, if you want a one-stop solution for going from Mountain View to Cupertino, this is your best bet. **Paul Taylor**

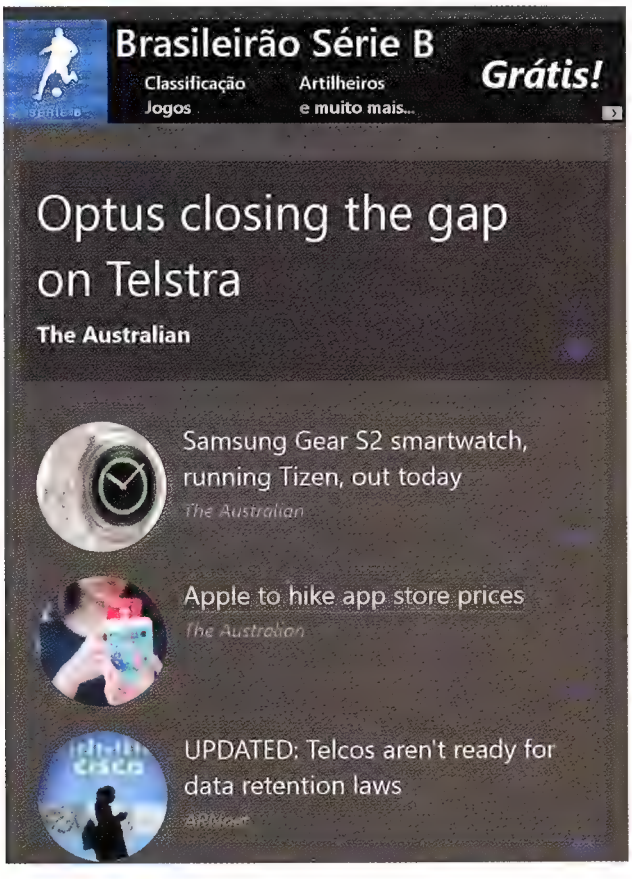

Transfer Complete
Your data has been copied to your new iPhone or iPad.
Some items were not copied, such as purchased apps or media, or media that is saved within apps.
Done
Recycle your Android Phone
You can recycle this Android phone for free at any Apple Store.

LeadStory

Your smartphone news anchor.

FREE; PRO, $1.19 | TINYURL.COM/APC422-LSTORY

Sadly, there aren't all that many RSS readers, news apps or dedicated magazine platforms available to Windows Phone users – and we don't foresee Apple News porting to Windows Phones anytime soon. As such, we were intrigued when LeadStory popped up on the Windows Phone app store. This news reader is powered by the Google News platform, so the content is quite good and should, in theory, get better as Google continues to develop it. You can also plug your location in so that LeadStory will show both national and local news, rather than its default US-centric collection of articles. With additional World, Tech, Entertainment and Science sections, the app does a commendable job of covering the biggest news of the day in all the key areas. The layout isn't overly refined, however, with the combination of white headlines on a grey background and circular images frankly looking a little dull – but you can open links to stories in your browser, so it's at least functional. If you want something in addition to Reddit to read news on your Windows Phone, then LeadStory isn't half bad – considering the lack of alternatives. Joel Burgess



Meme Generator Suite

FREE | TWITTER.COM/MEMEGENSUITE

The things that end up going viral on the internet are varied and unpredictable, but if you want to have a good crack at making your own web sensations, having a meme generator could be a decent way to earn some online kudos. Meme Generator Suite is a free app with a paid Pro tier that allows you to quickly make memes from an enormous selection of new and popular images, or using your own photos from your smartphone. You can also tap into the massive archive of memes on memegenerator.net by searching for specific images using the site's database. The editing page allows you to tweak the size, colour and positioning of text on a template image and then quickly share it through a number of compatible social apps. Although you'll mostly need to have a data connection to use it, the app also allows access to a number of background images while offline, so you won't miss a chance to insert your social commentary — even if you're temporarily offline.
Joel Burgess

Pocket Rally

$1.19 | TINYURL.COM/APC422-POCK

This rally game is definitely one of the more enjoyable driving titles we've come across on the Windows Phone Store. Using the touchscreen to accelerate and brake and the smartphone's orientation to turn the car, the simple controls are easy to comprehend but difficult to master. The first few rounds are a little tricky to overcome, but as you get used to the timing of the steering and when to use the throttle, that learning curve thankfully flattens off a bit. Powered by the Unity engine, the graphics aren't too bad either, with impressive looking rally-cars and realistic-but-simple backgrounds adding up to make the core experience a visually enjoyable one. The game can get a bit repetitive, as there are only eight playable cars and eight tracks, but the minimalist approach has also allowed the creators to focus on the level design and integrate subtly difficult obstacles into each raceway. The challenges fluctuate between single lap, double lap and opponent time trials and will make you redo each track in various cars.
For $1.19 this is an entertaining game that'll likely keep you occupied for hours.
Joel Burgess

techradar.

The home of technology

techradar.com

DIGITAL PRIVACY & SECURITY

REVEALED: WHAT THE REAL THREATS ARE + HOW TO PROTECT YOURSELF ON *ALL* YOUR DEVICES

38 THE REAL THREATS REVEALED
There are myriad menaces to your digital security in 2015. We explain what you need to be wary of in this in-depth Q&A.

42 THE BEST SECURITY SUITES FOR WINDOWS
We compare the current top 10 security suites for locking down your Windows PC , laptop or tablet.

49 SECURITY ON MAC (AND WHY YOU NEED IT)
We investigate OS X security and discuss why the built-in bits might not always be enough.

52 IS ANDROID SECURITY AS DIRE AS IS SEEMS?
The critical info you need to know about protecting your Android smartphone or tablet.

59 SECURITY ON iPHONE & iPAD
Apple's mobile devices aren't impervious to attack. Here's the info you need to safeguard your iOS device.

60 SMARTER PASSWORDS MADE EASY
We test nine easy-to-use password managers to find out which offer the best mix of usability and security.

64 PROTECT YOUR PRIVACY WITH A VPN
With the new metadata retention laws, it's time to take your online privacy into your own hands.

The real threats revealed

There are myriad menaces to your digital security in 2015. Nathan Taylor explains what you need to be wary of in this in-depth Q&A.

If you've been reading APC for a while now, you've probably got most of the basics of computer security down. Install a suite, use good passwords, be careful about who you trust online. Instead of rehashing the basics, we thought we'd look at some of the deeper answers to the questions you've asked us: the motives of virus makers; the security of social media and browser password managers and the need for security on other devices.

WHAT DO CYBER-CRIMINALS REALLY WANT?

Money. OK, sometimes not money. But mostly, money.

The popular image of the hacker and malware writer as the anti-government anarchist or capricious nerd doing it for the lulz is one that has long since passed its use-by date. Most cyber crime is the work of criminal gangs that produce malware as a means to make money.

Typically, these groups seek to acquire revenue in one of four ways:

- **CREDIT CARD INFORMATION AND IDENTITY THEFT.**

Spyware installed on the victims' computers is used to gather financial information that can be appropriated by the criminals. Alternatively, they use social engineering like phishing scams to get people to willingly hand over financial data.

- **RANSOMWARE.**

This has seen something of a resurgence of late. At its most benign, it's simply scareware – telling you that you have a virus and you need to install an app to remove it. In some cases it might turn off certain system features and demand money to turn them back on – which can often be easily bypassed by using Windows Safe Mode and performing a system restore.

The most vicious ransomware viruses typically encrypt all or part of your hard drive, preventing access to your files. The only way you can get your photos and documents back is to pay the criminals. The Cryptolocker virus and its imitators (like Crowti and Tescrypt) are the most common current ransomware; they search your hard drive and encrypt files of certain types (including Office documents and pictures), demanding money if you want them decrypted.

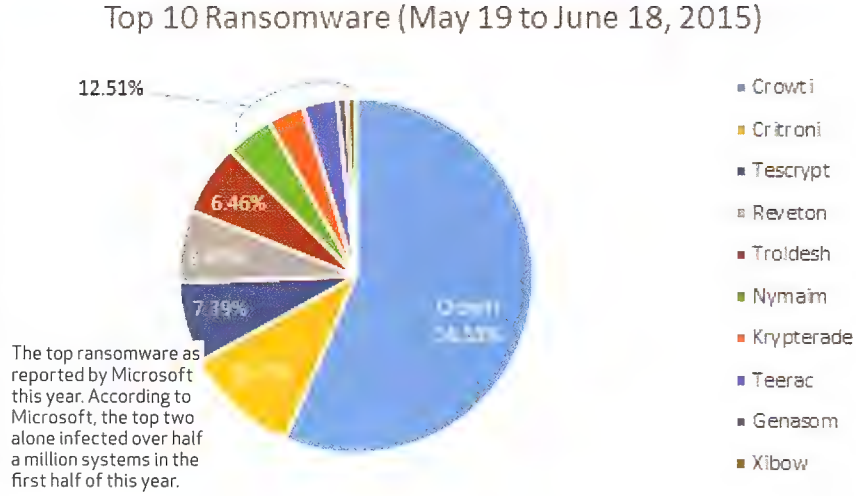
The original Cryptolocker was actually shut down last year (and the decryption keys made available to the public so if you lost data it could be restored), but a number of clones have popped up and are making the rounds right now.

- **ADWARE AND BROWSER HIJACKERS.**

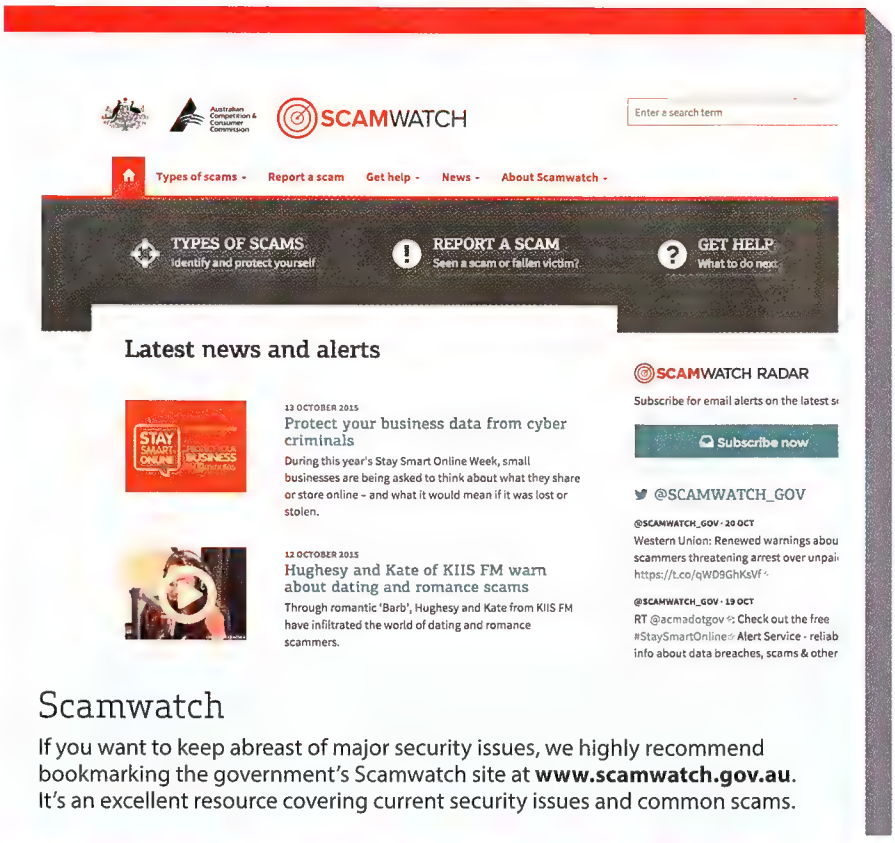
This kind of malware forces you do download ads supplied by the criminal, creating page impressions (and thus revenue) on the particular ads. It takes a number of forms, from actual browser hijacks to more subtle systems that redirect ad requests you'd normally get when browsing to ads supplied by the malware. Unfortunately, many hijackers are not officially classified as malware (since they're often sideloaded with other apps and you technically have an opt out during installation, if you paid attention), so anti-virus tools often don't remove them – you have to do it manually.

Your personal files are encrypted!
Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site
and follow the instruction.
in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.42k2bu15.com
https://34r6hq26q2h4jkzj.tor2web.blutmagie.de
Use your Bitcoin address to enter the site:
Click to copy address to clipboard
if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address 34r6hq26q2h4jkzj.onion
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.
Your private key will be destroyed on:
4/13/2015
Time left: 00:00
Click for Free Decryption on site
Show files
Enter Decrypt Key

The splash screen of cryptographic ransomware.



The top ransomware as reported by Microsoft this year. According to Microsoft, the top two alone infected over half a million systems in the first half of this year.


SCAMWATCH
Enter a search term
Types of scams
Report a scam
Get help
News
About Scamwatch
TYPES OF SCAMS
Identify and protect yourself
REPORT A SCAM
Seen a scam or fallen victim?
GET HELP
What to do next
Latest news and alerts
13 OCTOBER 2015
Protect your business data from cyber criminals
During this year's Stay Smart Online Week, small businesses are being asked to think about what they share or store online – and what it would mean if it was lost or stolen.
12 OCTOBER 2015
Hughesy and Kate of KIIS FM warn about dating and romance scams
Through romantic 'Barb', Hughesy and Kate from KIIS FM have infiltrated the world of dating and romance scammers.
SCAMWATCH RADAR
Subscribe for email alerts on the latest s
Subscribe now
@SCAMWATCH_GOV
@SCAMWATCH_GOV · 20 OCT
Western Union: Renewed warnings abou
scammers threatening arrest over unpai
https://t.co/qWD9GhKsVf
@SCAMWATCH_GOV · 19 OCT
RT @acmadotgov: Check out the free
#StaySmartOnline Alert Service - reliab
info about data breaches, scams & other

Scamwatch

If you want to keep abreast of major security issues, we highly recommend bookmarking the government's Scamwatch site at **www.scamwatch.gov.au**. It's an excellent resource covering current security issues and common scams.

"The popular image of the hacker and malware writer as the anti-government anarchist or capricious nerd doing it for the lulz is one that has long since passed its use-by date."

■ **BOTNET RENTAL.**

Zombie Trojans infecting large numbers of computers allow cyber-criminal to sell mass computing power – typically to other criminals, who might use it for denial of service attacks, spam propagation and to infest even more computers with spyware or ransomware. The ZeuS botnet and its successors are the most famous examples of this kind of operation.

Of course, there are other cyber-criminals that aren't motivated directly by money. Tools like Low Orbit Ion Cannon allow just about anybody to run denial of service attacks, while dictionary and brute force password crackers like Hydra can be used to access cloud services and private networks. These tools can and have been used to create chaos just for the "fun of it", to make some political point, or to access restricted files – and such attacks still happen with disturbing regularity.

Then there is malware developed as a mechanism for cyber-warfare. The most famous example is Stuxnet, allegedly a joint American-Israeli product designed to attack Iran's nuclear facilities but later repurposed and potentially used in criminal activities.

And finally there is the commercial malware, malware typically produced to prevent or punish copyright infringers – a practice that goes back to the very first virus, Brain, and includes efforts like Sony putting the XCP rootkit on its music CDs in 2005. Thankfully, at least in this last area, corporations have learned their lessons and such malware is very rare now.

THE INFORMATION YOU SHOULDN'T SHARE ON SOCIAL MEDIA

It's tempting to say, "don't share anything at all," but let's be realistic: you'll probably want to post something.

From a security perspective, it's always a good starting point to think that anything you post to Facebook or Twitter is now public information, privacy settings notwithstanding. Given that, you should never share:

■ Personal phone numbers, email

Top 10 digital security mistakes you're making

Thinking that installing a security suite is all you need. A suite is a good start, but it's not the end-all of security.

■

Not taking advantage of two-factor authentication. It's available for most major sites now: use it.

■

Not backing up on schedule. It's so easy to set up now.

■

Open email attachments without authenticating their source (if it appears to be from someone you know, email them back asking if it's real if you're at all unsure).

■

Insecure admin access to your PC or phone. Add a password/lock screen.

■

Poor passwords/using the same password for multiple things. This is where password managers come in really handy.

■

Insecure data storage. Keeping and carrying around data on an unencrypted flash or portable hard drive is just begging for it to be stolen.

■

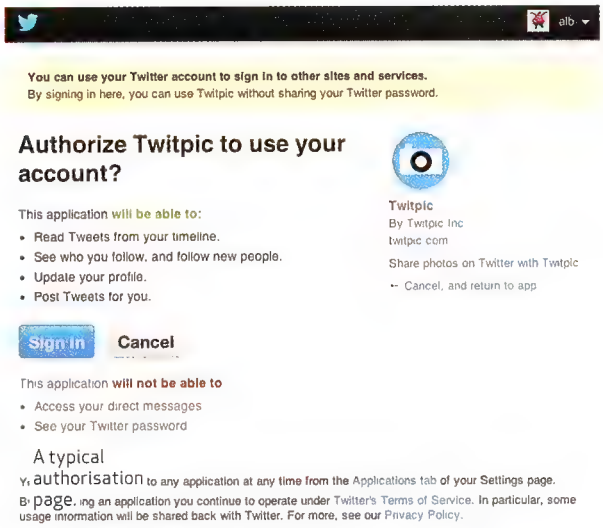
Not using a VPN on public Wi-Fi networks. If you're connected to a public Wi-Fi network, you're essentially on the same LAN as everybody else on that network. Use a VPN to secure your transmissions.

■

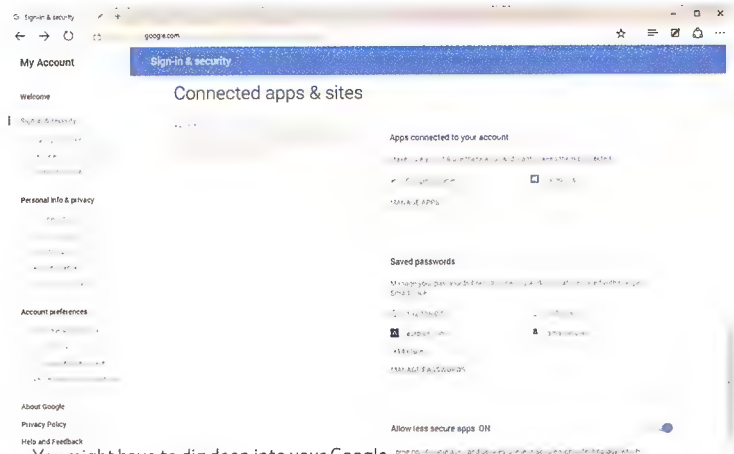
Never testing your backups. Make sure they're working occasionally. Just in case.

■

Not being careful about where you surf and what you download. Treat your computer like a temple. If you invite the bad element in, it's hard to get it out.


You can use your Twitter account to sign in to other sites and services.
By signing in here, you can use Twitpic without sharing your Twitter password.
Authorize Twitpic to use your account?
This application will be able to:
Read Tweets from your timeline.
See who you follow, and follow new people.
Update your profile.
Post Tweets for you.
Twitpic
By Twitpic Inc
twitpic.com
Share photos on Twitter with Twitpic
Cancel, and return to app
Sign in
Cancel
This application will not be able to
Access your direct messages
See your Twitter password
authorisation to any application at any time from the Applications tab of your Settings page.
page. ing an application you continue to operate under Twitter's Terms of Service. In particular, some usage information will be shared back with Twitter. For more, see our Privacy Policy.

A typical



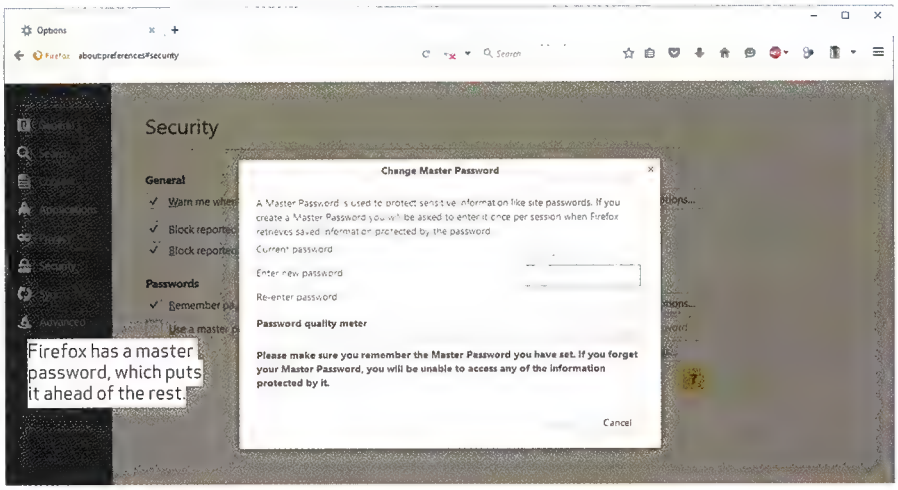
You might have to dig deep into your Google, Facebook or Twitter account settings to find and disable social logins from specific sites and apps.

addresses and home addresses.

- Social engagement and vacation details.
- Financial information (even what bank you're using).
- Driver's license details.

There's a second tier of things you should be careful about as well: things that might be used to bypass authentication checks. Commonly, authentication checks ask for things like: your date of brith, your first pet's name, your mother's maiden name and the street you grew up on. Whenever you're asked to set up such an authentication question, you should check social media to see if you've ever posted the answer to those questions.

And finally, there's just embarrassing stuff that you may think is fun but can actually be harmful to your image. There's a roughly 100% chance that a prospective employer is going to check your social media accounts, and any drunken hijinks, nude selfies or complaints about former employers may come back to bite you.


Options
about:preferences#security
Security
General
Passwords
Change Master Password
Password quality meter
Please make sure you remember the Master Password you have set. If you forget your Master Password, you will be unable to access any of the information protected by it.
Cancel
Firefox has a master password, which puts it ahead of the rest.

INSTANT LOGINS: IS SIGNING IN VIA YOUR GOOGLE, FACEBOOK, MICROSOFT OR TWITTER ACCOUNT SAFE?

An awful lot of apps and sites now use what is called a "social login". In lieu of the usual username and password, they give you the option to "sign in with your Facebook/Twitter/Google/Microsoft/whatever account." On the surface, it seems like a convenient thing – it's one less password that you have to manage. Instead, you can bundle all your site logins into one social networking login. Once you're logged into, say, Facebook, you're effectively logged into all the sites that you use Facebook to log into.

You may be wondering: is this safe? The answer is, unfortunately, a little more complex than a simple yes or no. It can be OK if you're careful, but dangerous if you're not.

The first time you click on such a link on a new web site, what will happen is that you'll be redirected to a page supplied by the social service you want to use to log in (Facebook, for example). There, you'll be asked if you want to allow that service to access the account. This is done via a protocol called OAuth.

So, let's say you'd like to access a site called siteiwant.com, and you try to log into it using your Facebook account. Siteiwant.com will sent an OAuth request to Facebook, and you'll be redirected to a Facebook page that asks if you'd like to give siteiwant.com access and will list the account details and elements that it would like access to. If you say yes, Facebook will send siteiwant.com a token that gives them access to your account information and any APIs that you've agreed to. From then on, as long as you're logged into Facebook, the site can automatically identify you and log you into the service, no password required.

OAuth will not send them your social password or login details , so they couldn't use this system to wholly hijack your Facebook account, which is no doubt some comfort. But there are security implications.

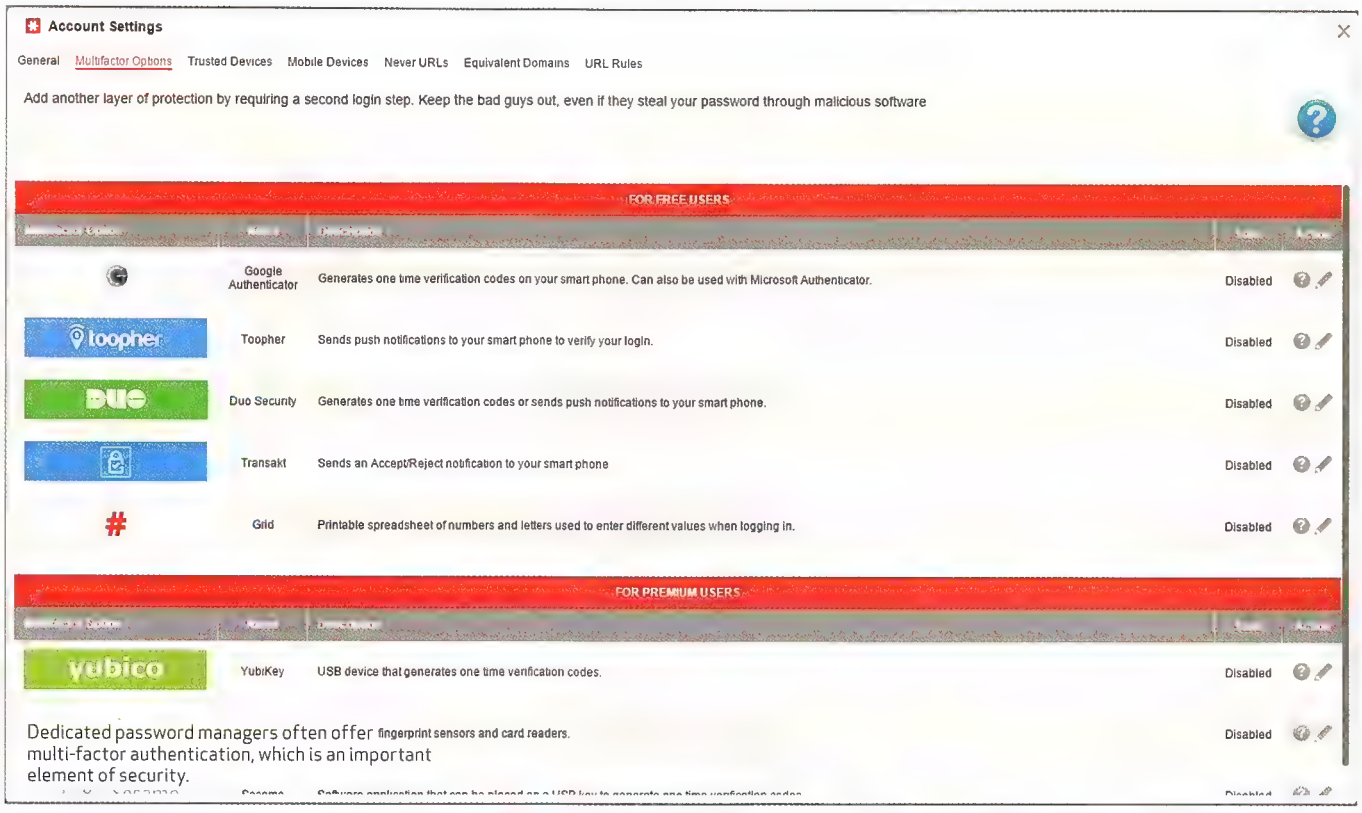
For a start, once a site receives permission from the social network to access the account, it retains that permission. The token is permanent, unless you specifically go into your social networking account and revoke it. It's a good idea to check your app and site permissions every now and then and revoke those you don't use.

Second, this links your site/app login to a specific social media account. The site will be able to very easily identify who you really are using that link, and potentially use that data to mine information about you. There will be very little to no anonymity with this login method.

Third, much like mobile app permissions, you may end up giving the site too much access to your social media account. If you're not paying attention on the agreement page, you may allow it to make Facebook posts, 'Like' things on your behalf, send Tweets, follow other people and more.

Finally, it's a single point of failure. If your social media account is compromised, a lot of other site logins are compromised as well.

Ultimately, it comes down to how much you trust the app or site provider. We absolutely wouldn't recommend using social logins on sites where you're not 100% sure of the legitimacy of the


Account Settings
General
Multifactor Options
Trusted Devices
Mobile Devices
Never URLs
Equivalent Domains
URL Rules
Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software
FOR FREE USERS
Google Authenticator
Generates one time verification codes on your smart phone. Can also be used with Microsoft Authenticator.
Disabled
toopher
Toopher
Sends push notifications to your smart phone to verify your login.
Disabled
DUO
Duo Security
Generates one time verification codes or sends push notifications to your smart phone.
Disabled
Transakt
Sends an Accept/Reject notification to your smart phone
Disabled
#
Grid
Printable spreadsheet of numbers and letters used to enter different values when logging in.
Disabled
FOR PREMIUM USERS
yubico
YubiKey
USB device that generates one time verification codes.
Disabled
Dedicated password managers often offer multi-factor authentication, which is an important element of security.
fingerprint sensors and card readers.
Disabled

provider. But if you feel comfortable with the site, and are careful about reading the permissions, then it should be OK for sites you trust.

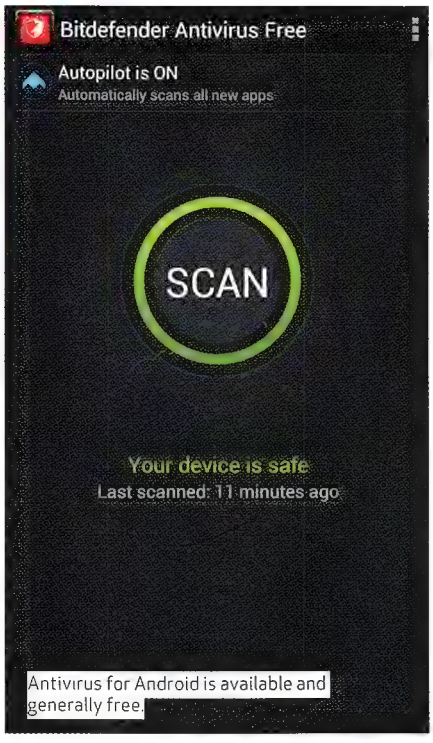
BROWSER PASSWORD MANAGERS: ARE THEY SAFE?

Whatever web browser you're using, there's a good chance it has an in-built password manager. You may be wondering if it's secure, and the answer is: probably not as secure as a dedicated password manager.

What browser password managers do is store your passwords in an encrypted file on your hard drive. If the browser offers password sync (like Chrome or Firefox), that encrypted file is uploaded in its encrypted form to a shared service – your Google Cloud Drive or the Firefox Sync servers. In general, syncing should be OK as long as you have a good password on your sync.

The biggest problem with browser-based password managers is that anyone who can log into your PC or mobile can see them all, without any further authentication required. Of course, they do need physical access to your PC or mobile, but once they have it, they have everything, since there is no master password by default – it's linked to your system or mobile login. A security tool like WebBrowserPassView (**www.nirsoft.net**) can extract them all in an instant.

One thing we should note is that Firefox actually deserves props here. Although it's not switched on by default, it does have the option of adding a master password. Head to 'Options › Security' and check the box to add it.


Bitdefender Antivirus Free
Autopilot is ON
Automatically scans all new apps
SCAN
Your device is safe
Last scanned: 11 minutes ago
Antivirus for Android is available and generally free.

Even Firefox is inferior to dedicated password managers like LastPass (**lasspass.com**), 1Password (**agilebits.com**) or KeePass (**keepass.info**), however. Most such dedicated password managers have a master password distinct from your Windows login, and they have other security tools, like password audits and auto-generation of good passwords. The cloud-based ones like LastPass and 1Password also support two-factor authentication, which is a huge security addition.

DO I NEED SECURITY ON MY OTHER INTERNET DEVICES?

Yes, on mobiles especially. While most internet-connected devices don't run services and are relatively safe behind a router firewall, your mobile is now essentially a PC in miniature. It can and will run hackable services and is vulnerable to Trojans and even things like email worms.

This is proving to be a particular problem on Android, especially where manufacturers are refusing to update the system software to the latest version (because they'd rather have you buy a new product than support the old one). Not even Google supports versions of Android prior to 4.3, and if you have a phone more than two years old good luck getting updates for it.

That leaves an awful lot of Android devices vulnerable to new exploits that will never get patched. Viruses like Stagefright 2.0 can easily exploit the holes in older devices.

That's why, especially on older Android devices, it's a very good idea to run anti-virus software – there are plenty of free apps available, and we've reviewed a wide selection on page 52. Also, make sure you only download apps from official sources like Google Play, and keep up all the good security practices you use on your PC – data security, lock passwords, anti-theft and backup. ■

The best security suites for Windows

Nathan Taylor compares the current top 10 security suites for locking down your Windows PC, laptop or tablet.

Although OS developers have gotten much better at security over time, hackers have also grown more savvy. Highly-organised criminal gangs have been very successful at continuing to find exploits – either through social engineering or holes in unpatched software.

So, even in 2015 and 2016, it's still a very good idea to have a security suite installed. Relying on Windows Defender and Windows Firewall alone is not enough. You need a comprehensive backup plan, you need filters that stop you and your family from accessing malicious or undesirable web sites, you need secure browsers for banking and file shredders for keeping your data private. It sucks, we know, but that's the reality of the internet.

This issue we've gone ahead and taken a look at our current top ten suites. Unfortunately we don't have space to review every suite on the market, but we took a look at the latest anti-malware test results and decided to evaluate those suites with the best results.

ABOUT THE TEST RESULTS

Each of the suites reviewed here has been comprehensively tested by independent antiviral analysis company AV-Test (**www.av-test.org**). We've published here the latest results available at the time of writing, from August 2015.

Note that the results are not, in all cases, from the specific products reviewed below. For example, we may have reviewed the full suite where AV-Test may have only tested the stand alone anti-virus application. That doesn't change the validity of the results, since the same anti-virus engine is in use.

Let's break down just what the numbers mean:

- Protection against 0-day malware attacks is a measure of the suite's ability to detect new viruses based on their behaviour. It's perhaps the most important number here.
- Detection of widespread and prevalent malware shows the detection percentage of known viruses released in the four weeks before the test.
- Performance impact is a measure of how much the suite affects system speed when visiting websites, downloading software, installing and running programs and copying data. Higher is worse (more impact).
- False warnings is the number of instances where the suite flagged legitimate software and web sites as a threat and either blocked it or produced a warning popup.

For convenience, AV-Test also provides three overall scores, rating each suite's protection, performance impact and usability out of six, to give a total score out of 18. (Usability, in this instance, is not a reference to ease-of-use, but is based on the number of times the program produced false

Glasswire does more than block intruders: it gives a complete picture of your net usage.

Roll your own suite for free

So you're not that keen on paying an annual subscription for protection from net nasties? Well, with a few free tools, you can build your own comprehensive set of protections for your system. Here are our current top picks for the free tools available for different security tasks:

ANTI-MALWARE: AVAST FREE ANTIVIRUS (WWW.AVAST.COM).
Still the best free anti-malware solution available, protecting you from both viruses and unwanted programs like browser hijackers. It also has a home network security scanner.

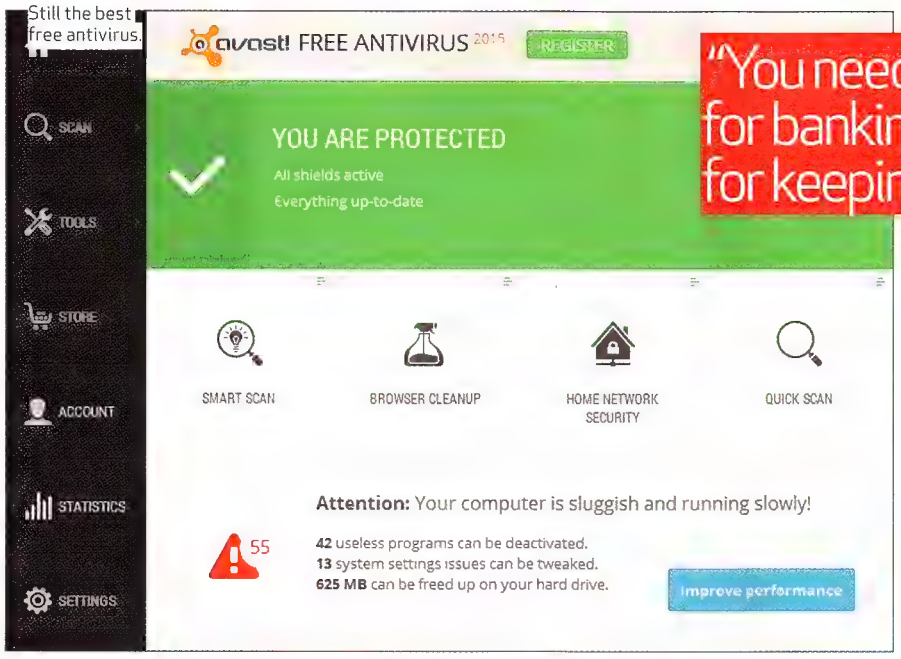
FIREWALL: GLASSWIRE FREE (WWW.GLASSWIRE.COM)
This one was tough – and frankly the built in Windows Firewall is actually pretty good. But if you want a bunch of extra traffic monitoring and reporting capabilities, GlassWire brings it. Traffic is broken down by volume, type and much more.

PASSWORD MANAGER: LASTPASS (WWW.LASTPASS.COM)
Cloud-based, with multi-factor authentication, the free version of LastPass doesn't have mobile device syncing and support, but it has just about everything else.

BACKUP: CODE42 CRASHPLAN (WWW.CODE42.COM)
Although it's linked to a paid cloud service, the actual CrashPlan backup app can be downloaded and used for free. And it's fantastic, allowing you to set up your own cloud of backups, including backing up to/from a friend or family member's PC over the internet.

PARENTAL CONTROLS: NORTON FAMILY
While the Premium version adds things like showing you snippets of the YouTube videos your kids are watching as well as Android mobile support, the free Norton Family version is still pretty darn great, with time supervision, web filters, social network monitoring and more.

ANTI-TRACKING: DISCONNECT FREE (DISCONNECT.ME)
An essential browser add-on that stops an awful lot of the crap that web sites try to pull. No tracking cookies, social media widgets, no logging of searches and a forced HTTPS connection where available.



"You need secure browsers for banking and file shredders for keeping data private."

popups and blocked legitimate software). We should note that AV-Tests aggregate scores are based on combined Jul-Aug performance, while we've only printed August results for space reasons.

While we've provided an extended table of results, we don't have room here to review every anti-virus product tested. We limited ourselves to the suites with the ten best results (AVG just squeaking in because it had a better protection score than the other suites that scored 16, as well as a perfect detection rate).

AV-TEST CONSUMER SECURITY SOFTWARE TEST RESULTS

TEST PERIOD: AUGUST 2015
TEST PLATFORM: WINDOWS 7, SP1 (64 BIT)

VENDOR	SPECIFIC PRODUCT TESTED	WEBSITE	PROTECTION AGAINST 0-DAY MALWARE ATTACKS	DETECTION OF WIDESPREAD AND PREVALENT MALWARE	PERFORMANCE IMPACT (HIGHER IS WORSE)	FALSE WARNINGS OR BLOCKAGES WHEN VISITING WEBSITES	FALSE WARNINGS ON INSTALLING NEW SOFTWARE	FALSE WARNINGS CONCERNING CERTAIN ACTIONS CARRIED OUT WHILST INSTALLING AND USING LEGITIMATE SOFTWARE	FALSE BLOCKAGES OF CERTAIN ACTIONS CARRIED OUT WHILST INSTALLING AND USING LEGITIMATE SOFTWARE	PROTECTION SCORE	PERFORMANCE SCORE	USABILITY SCORE	TOTAL SCORE
AHNLAB	V3 Internet Security 9.0	www.ahnlab.com	100%	100%	5	0	10	0	0	6.0	3.5	4.5	14.0
AVAST	Free AntiVirus 2015	www.avast.com	100%	100%	3	0	0	0	0	5.5	4.5	6.0	16.0
AVG	Internet Security 2015	www.avg.com	100%	100%	4	0	3	0	0	6.0	4.0	6.0	16.0
AVIRA	Antivirus Pro 2015	www.avira.com	100%	100%	2	0	0	0	0	6.0	5.0	6.0	17.0
BITDEFENDER	Internet Security 2015	www.bitdefender.com.au	100%	100%	0	0	0	0	0	6.0	6.0	6.0	18.0
BULLGUARD	Internet Security 15.1	www.bullguard.com	99%	100%	2	0	8	0	0	6.0	5.0	5.5	16.5
COMODO	Internet Security Premium 8.2	www.comodo.com	100%	94%	1	0	1	0	3	3.0	5.5	5.5	14.0
ESET	Smart Security 8.0	www.eset.com	95%	99%	6	0	1	0	0	5.0	3.5	6.0	14.5
F-SECURE	Internet Security 2015	www.f-secure.com	100%	100%	1	0	4	0	0	6.0	5.5	5.5	17.0
G DATA	InternetSecurity 2015	www.gdatasoftware.com	95%	100%	8	0	1	0	0	5.5	3.0	6.0	14.5
K7 COMPUTING	TotalSecurity 15.1	www.k7computing.com	99%	100%	3	0	7	0	0	6.0	4.5	5.5	16.0
KASPERSKY LAB	Internet Security 2016	www.kaspersky.com	99%	100%	0	0	0	0	0	5.5	6.0	6.0	17.5
MCAFEE	Internet Security 2015	www.mcafee.com	99%	100%	1	0	0	0	0	6.0	5.5	6.0	17.5
MICROSOFT	Security Essentials 4.8	www.microsoft.com	87%	100%	2	0	2	0	0	3.0	5.0	6.0	14.0
MICROWORLD	eScan internet security suite 14.0	www.microworld.com	96%	100%	3	0	0	0	0	5.5	4.5	6.0	16.0
NORMAN	Security Suite Pro 11.0	www.norman.com	92%	100%	4	0	0	4	2	5.0	4.0	5.5	14.5
PANDA SECURITY	Free Antivirus 15.1	www.cloudantivirus.com	100%	100%	2	0	0	0	0	6.0	5.0	6.0	17.0
QIHOO 360	360 AntiVirus (BD+QVM) 5.0	http://sd.360.cn/download_center.html	99%	100%	4	0	0	0	0	6.0	4.0	6.0	16.0
QUICK HEAL	Total Security 16.0	www.quickheal.com	91%	100%	8	0	1	1	2	4.5	3.0	5.5	13.0
SYMANTEC	Norton Security 2015	www.symantec.com	100%	100%	2	0	4	0	0	6.0	5.0	5.5	16.5
TREND MICRO	Internet Security 2016	www.trendmicro.com	100%	100%	2	0	3	0	1	6.0	5.0	5.5	16.5

$90 FOR 3 PCS FOR 1 YEAR | WWW.AVG.COM

AVG Internet Security 2016

User friendly, but not all that remarkable.

Touch screen friendly and very easy to use, AVG Internet Security has a number of little details that recommend it. Not enough to recommend it over BitDefender or Kaspersky, but you're certainly not buying a dud with AVG.

From a usability standpoint, it couldn't be much easier. Most of the user settings are of the on-off variety, while most of the mechanics of protection are handled behind the scenes. There are annoyances, like the use of a stub pre-installer which doesn't download the app until you start installation, but they're manageable.

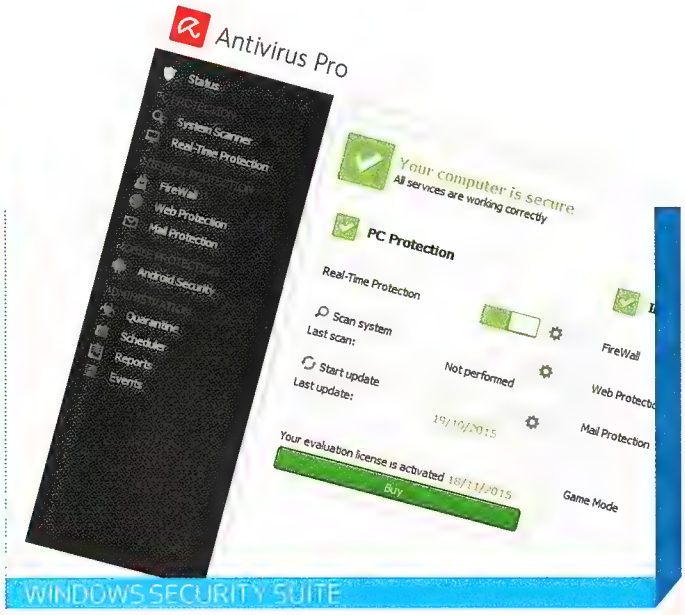
Its feature set covers all the basics: your email protection, firewall, phishing, web site and link scanner and anti-malware. There is no parental control, secure browser or sandbox environment. There are some utilities built in, like a PC "tuneup", including registry fixer, defragger, junk file remover and file shredder – all fine, but nothing special. Indeed, average is really the way to best sum up this suite – its features aren't terrible, but they're not remarkable either. The one notable thing it has is a drive encryption tool, allowing you to create a special protected virtual drive for important files. It's very useful, but probably not enough to recommend AVG over higher ranked suites.

Its anti-malware performance results put it just inside our top ten suites. The detection rates were stellar across the board, hurt only by a handful of false positive. It detected every virus thrown at it. Its biggest issue was its performance, with AV-Test finding that it had a notable impact on system performance when running.

Verdict

It's affordable and wonderfully easy to use, but otherwise does nothing to stand out from the pack.

★★★½☆



$93.95 FOR 3 PCS FOR 1 YEAR | WWW.AVIRA.COM

Avira Internet Security

A retro suite with some nice touches.

A security suite with a decidedly retro design and feature set, Avira is distinguished by an excellent anti-malware engine and multi-device management.

Initially, the internet download process just installs the anti-virus tool, and then you have to load the additional modules into it to turn it into the suite. These appear as buttons on the bubble that pops up when you click on the taskbar icon, each button launching a discrete app: one for anti-virus, one for system tuning (defragging and junk removal), one for browser protection, one for identity protection and one for anti-theft. There's little to no integration between these elements, and none of them is touch screen friendly at all.

Still, there are some genuinely cool elements hidden through the apps. Avira aggressively removes potentially unwanted apps from your system, cleaning out things like browser hijackers that might not technically be viruses, but they are damned annoying. It has a neat little file encryption app and a rather strange but quite cool online price comparator.

Our favourite feature of the suite, however, may be the web-based device management console, which lets you view the reports from all the Avira installations attached to your account. It's not a full web service like you might find in a corporate tool (you can't actually do much to change the settings on the PCs), but it's a very useful way of getting a snapshot of any security problems on your network.

Verdict

It's a little disjointed, and the interface is old school, but there are clever features built in.

★★★½☆

$99.95 FOR 3 PCS FOR 1 YEAR | WWW.BITDEFENDER.COM.AU

Bitdefender Internet Security

Pretty close to perfect.

For some years now, Bitdefender's boasted the best performance and features in a security suite. As the editor's choice for this review, it has everything: perfect anti-virus test results, an incomparable set of security features, very little impact on system performance and a one-click security model that's perfect for beginners.

This latest version of Bitdefender retains the complete feature set we've lauded in the past: excellent anti-malware, firewall and web protection, as well as email plugins for anti-spam and anti-phishing. There's a safe browser for online banking, a file shredder and a pretty decent (though a little confusing at first) password manager. Paying an extra $30 for the Total Protection version adds file encryption, system tune-up and anti-theft.

The suite also boasts a first: anti-ransomware to combat the current plague of infections. Although switched off by default, it lets you lock selected files and folders, preventing them from being encrypted by a third-party app.

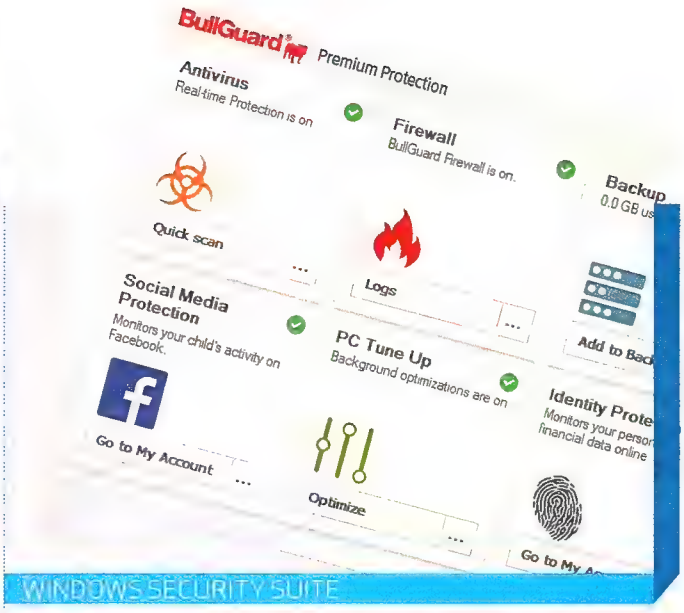
Finally, there's now Bitdefender Central, a cloud service that lets you see the security on devices attached to your license. It can be used to remotely initiate scans and is now the central location for managing the outstanding new parental control features, which are second only to Symantec's.

In short, Bitdefender is absolutely everything we want in a suite. It covers all your bases and does everything pretty well. In autopilot mode it almost never bothers you, and is the very best you can get right now.

Verdict

Pretty much perfect.

★★★★★



$89.95 FOR 3 PCS FOR 1 YEAR | WWW.BULLGUARD.COM

Bullguard Internet Security

A suite with a broad but shallow set of features.

Although it may not be a suite that many Australians know, Bullguard has once again drawn our attention with impressive test results. It didn't produce perfect results for AV-Test, and there were too many false warnings on legitimate software (it's a little popup-happy), but its overall detection rates were very good.

The rest of the feature set feels broad, but a little shallow in places. It ticks a lot of boxes: online backup, firewall, anti-spam, web monitoring, PC tuneup and a few others, but some of those features are a little light, a little cursory.

That can't be said for its excellent parental controls, however. You can block access to site categories, monitor Facebook posts, manage application access and limit time online. Reports of child activity are available online, through your account pages on Bullguard's site. We'd put Bitdefender and Symantec's solutions ahead of it, but it's still a high point of the suite.

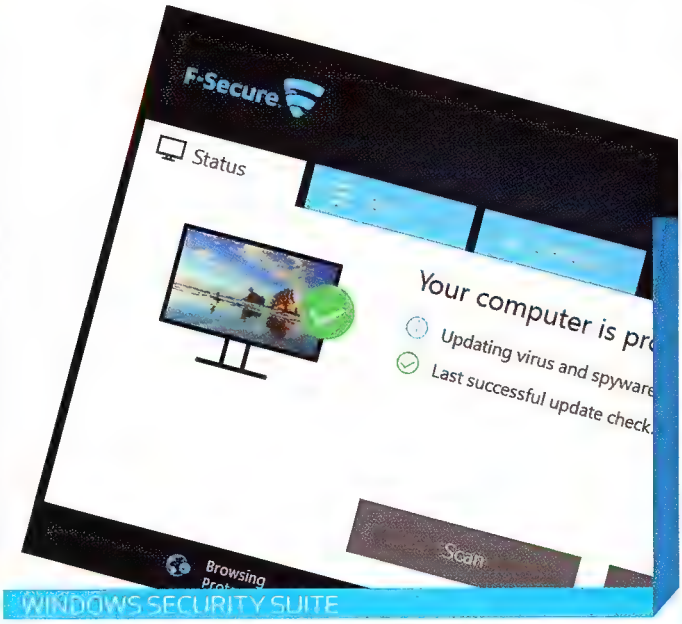
The suite's interface could still use some work. It can't seem to decide between the all-there-in-front-of-you approach of a Kaspersky or Avira and the keep it simple approach of AVG or Bitdefender. So it ends in a weird place that's perfect for neither beginners nor experienced users. It's also noisy, popping up too often to bother you with questions it should know the answer to.

Ultimately, this is another mid-level suite. It's still not truly competitive with the Kasperskys, Nortons and Bitdefenders in terms of features or ease of use. It has gotten better, and its test results are definitely notable, but it's not a top pick.

Verdict

A mid-tier suite, with solid anti-virus but relatively underpowered additional features

★★★



$93 FOR 3 PCS FOR 1 YEAR | WWW.F-SECURE.COM

F-Secure Internet Security

A solution that's starting to fall behind.

Where other companies like continue to innovate – even in the rather staid world of security software – F-Secure seems stuck in a rut, changing little from year to year. It's not that it's a bad suite – far from it – but it feels like it's starting to fall behind.

Let's start with the good: the test results. F-Secure has maintained its record of excellence when it comes to anti-malware, with a 100% detection rate and modest impact on performance. Its web filter was a little zealous, but that's nothing to worry about.

It's the rest of the suite that's uninspiring. The feature set is basic but solid, with a firewall, browsing protection, capable category-based parental controls, spam filter and online banking protection. A lot of extra features are available with add-ons: Booster (system and battery optimisation), F-Secure Key (password manager), Freedome (VPN) and Adblocker. The thing is, the full versions of most of these cost extra, when the cost of the suite should really cover them.

In addition, instead of a conventional installer, F-Secure uses a cumbersome web-based license system that requires you to download and install an app in order to download the other apps. While we can see the value of this for multi-platform setups, if you just want to install it on a single system it's an utter pain.

When it comes down to it, while we appreciate how good the anti-malware is, the rest of the base suite seems hardly worth the hassle, especially when better options are available.

Verdict

Excellent anti-malware as always, and snappy and easy to use as well. But the licensing system is a mess.

★★★☆☆

$99.95 FOR 3 PCS FOR 1 YEAR | WWW.KASPERSKY.COM

Kaspersky Internet Security

The second-best suite around.

For the past few years, the battle for best security software provider has seemed like a brawl between Kaspersky and Bitdefender. Other suites have proven somewhat competitive, but really the tussle for top spot remains between these two players.

This year, again, we felt that Kaspersky is just a little behind Bitdefender when it comes to both features and anti-malware.

On the latter, Kaspersky had one small hiccup in the 0-day tests preventing it from getting a perfect score across the board. Otherwise, the results were perfect, with no false positives and little impact on performance. Only Bitdefender got a better score.

When it comes to features, Kaspersky continues to innovate with the best. This suite that does an awful lot behind the scenes. There are privacy and web protections, category-based parental controls, a secure browser for online banking, webcam protection, a virtual keyboard to foil keyloggers and much more. If you're willing to fork out $20 more for the Total Security version, you'll also get a password manager with syncing across devices as well as a backup solution.

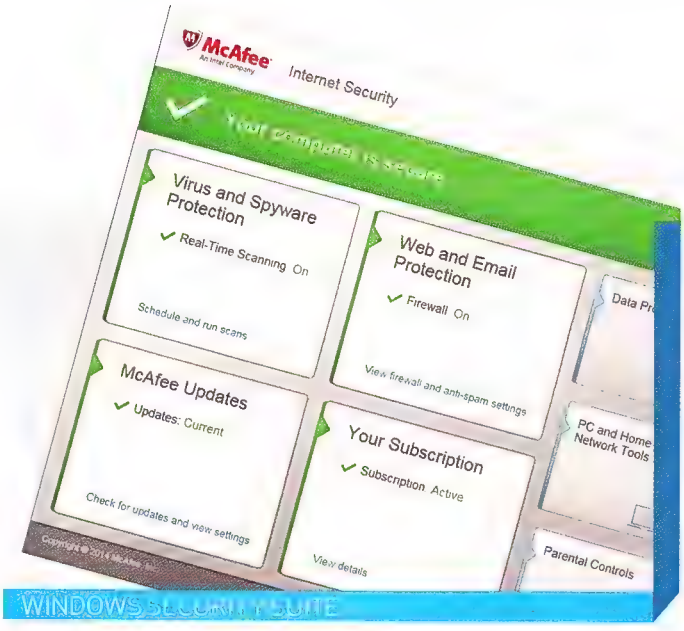
The interface keeps these depths well hidden until they're required, and the PC interface even has a convenient chat button if you want to talk to a real person for tech support. It's all very clean, though menu options and buttons are often too small to easily tap.

It's really another fantastic iteration of the suite. While not that many features have been added in this year's release, this was already an incredibly good suite and a top buy.

Verdict

Second only to Bitdefender in terms of overall quality. Excellent features and top performance.

★★★★½



$99.95 FOR ALL DEVICES OF A SINGLE USER | WWW.MCAFEE.COM

McAfee Internet Security

Some standout features mark this as a top suite.

Since coming under Intel's umbrella, McAfee had made a number of changes to its suite, none more notable than streamlining the interface into a simplified (mostly) touch-friendly affair that doesn't ask too many questions or demand too much from the user. Like the other top suites, it does most of its work behind the scenes.

There's a decent amount going on, too. Let's start with the anti-malware, which has improved dramatically in recent years. This year, it was a match with Kaspersky, missing one 0-day virus but otherwise having a perfect detection rate. Its impact on performance was minimal, and it was just 0.5 off the perfect 18 score (only Bitdefender scored 18).

It has a handful of really standout features as well. True Key, the password manager, is an outstanding solution, with two-factor authentication including face recognition. The web filter and anti-phishing tool is also best-in-class, proactively blocking dangerous links before you even click on them. The other core features: anti-spam, firewall, file shredder and a few others are solid if uninspiring, although we do have to say that the parental controls seem a little weak.

We're fans of McAfee's licensing model, which is a simple "once license for all the devices of a single user." That means a license lets you install McAfee on all the PCs, Macs and mobiles you own, without limit. Internet Security only comes with a single user license for True Key; but if you're willing to fork out an extra $30 for the Total Protection version, you'll get five, as well as a file encryption tool for theft protection.

Verdict

Outstanding anti-malware, web protection and password management.

$101.63 FOR 3 PCS FOR 1 YEAR | WWW.PANDASECURITY.COM

Panda Global Protection 2016

Clunky interface and management is rescued by some excellent features.

A suite with surprising breadth, Global Protection from Panda covers off a lot of threats. It can be rough around the edges, especially in terms of management, but it's a capable suite without glaring issues.

It ticks off a lot of boxes when it comes to features. There's general stuff, of course: the firewall, anti-spam and anti-malware. There's also a password manager, file encrypter, parental controls, a file shredder, tuneup, online backup, virtual keyboard, boot drive and Wi-Fi check for just a start. While it covers a lot, none of its features really stood out as particularly good or bad. There was one thing we were really impressed by, however: the Data Shield. Similar to Bitdefender's solution, it locks selected files and folders for protection against ransomware.

We aren't all that impressed with Panda's interface and management. It has gone full Modern UI, modelling the entire interface on Windows' Start Screen/Start Bar. This would make it great in a touch screen environment, except for all the popup windows it generates, which kind of defeats the purpose. It also inexplicably starts with a whole set of features not yet installed and disabled, and important features have to be manually downloaded and configured before they're active.

Still, it's an impressive suite overall, and one that produced absolutely perfect detection rates in AV-Test's benchmarks. Its system performance impact hurt it, but you can't fault it for protection.

Verdict

We don't love the interface, but virus-detection is excellent and there's a huge set of tools here.

$100 FOR 3 PCS FOR 1 YEAR | WWW.NORTON.COM

Symantec Norton Security Premium

In one word: elegant.

This year, Symantec has (thankfully) rationalised its security suite offering down to what's essentially a single product: Norton Security Premium, available for one, three or five devices. Security Premium is essentially the evolution of Norton 360, and it's certainly a major contender, up there with Kasperky and Bitdefender for quality.

It doesn't quite have their anti-malware chops. It did boast a perfect detection rate, but at the cost of too many false positives and a too much impact on system performance. It's excellent, but can be a bit annoying.

The real strength of the suite is in the care it's taken with the other security features. The identity theft protection and password manager are elegant, and the integrated backup solution – which can back up locally or to the 25GB of cloud storage that comes with the subscription – is great. It can be configured to run on a schedule or automatically back up during idle PC times. The system utilities are a little generic, but we do like the startup manager for controlling what starts when Windows does.

Like Bitdefender and Avira, the suite has a cloud service accessed through the Norton web site. Primarily this is for adding devices and licenses, but it's also where you manage Norton Family. These parental controls require a separate download and install on the kids' PCs and devices, but give excellent accounting and management of their online activity and you can manage their access through the web console. It's a true highlight of the suite, the absolute best solution on the market.

Verdict

Wonderful parental controls, included cloud backup and very good virus protection.

★★★★½

$59.95 FOR 3 PCS FOR 1 YEAR | WWW.TRENDMICRO.COM.AU

Trend Micro Internet Security 10

Perfect for families and non-technical users.

Trend Micro's cut-rate option for home users is an affordable way to get some comprehensive security coverage. Trend Micro offers more complete options: Maximum Security ($79.95 for four devices) and Premium Security ($149.95 for six devices), but if you already have a password manager and a mobile suite, Internet Security should be all you really need.

The suite's interface is as simple as can be. It opens with a big scan button, while side buttons allow for quick system health checkups and access to the suite's deeper features. Everything is prefaced and guided by a helpful tutorial system that explains features as you try to access them.

Trend Micro's privacy scanner is a highlight, with a web filter and link scanner for social media sites that pre-emptively warn against unsafe links. Data theft protection lets you configure certain phrases or numbers (like credit card numbers) that the suite won't transmit without a password. The parental controls are also worthy additions, with time and category-based restrictions on access. It doesn't have the excellent reporting tools of Symantec and Bitdefender, but it's still a good solution for families.

And that's really where this suite is targeted. Trend Micro's done everything in its power to keep things easy. The interface is non-threatening, the options simple and the features straightforward. If you're willing to pay extra, it even offers an additional IT help desk service. This accessibility is its greatest virtue, combined with security sufficient to protect you from most threats.

Verdict

Affordable and easy-to-use. Not as big as some of the competition, but it should be enough.

★★★★

Security on Mac (and why you need it)

Matthew JC. Powell investigates the current state of built-in OS X security and discusses why that might not always be enough.

Apple has taken some very serious steps in the last few versions of OS X to beef up its security, and OS X 10.11 – El Capitan – is no exception. In fact, the steps it has taken with El Capitan may be the boldest yet.

El Capitan features "System Integrity Protection" which prevents any software you install and run on your Mac, regardless of where you got it, from modifying the System itself or any of the applications and utilities that ship with OS X in any way. Point blank.

That means, of course, that a lot of utilities and customisation tools that Mac users have used and in some cases relied upon for years no longer work – because they need to modify components of the System. That's the price of security.

El Capitan also runs by default in "rootless" mode – that is, the "root" level of user access that's generally present in Unix-based operating systems is not present in El Capitan. This means that the "holy grail" of malware authors – gaining root access and control of your system – is simply not possible.

At least until someone figures out a way to do it. Which, in all probability, someone will eventually.

The above features of El Capitan are in addition to other OS X security features such as Sandboxing, Gatekeeper and the Application Firewall. There's also built-in anti-virus, and anti-phishing features in Safari (as well as just about any other OS X web browser).

If you make use of these features, and also install software only from the Apple App Store or trusted developers, you've got yourself a pretty secure system. So the question is, do you actually need anything more?

If and only if you don't do a lot of web browsing or downloading stuff, and your online interactions are only with other Mac users, you probably don't need to spend more money on security.

Otherwise yes, you do. Apple's included malware protection and firewall are good enough for a lot of users most likely, but they're very basic. For example, the firewall doesn't monitor outgoing traffic, only incoming – so if there's something spying on you you won't know. For another, the included AV doesn't look for Windows or Linux malware, only for nasties written specifically for OS X – so your machine can be used as a vector to infect others.

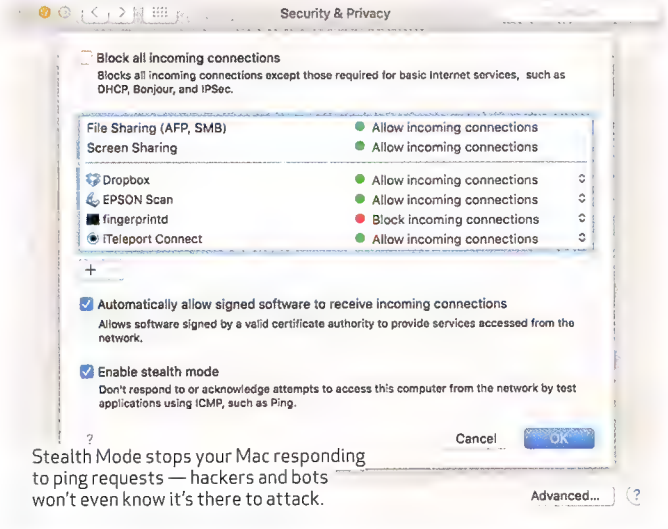
Lock down your Mac

There are a few simple steps you can take to boost security on your Mac.

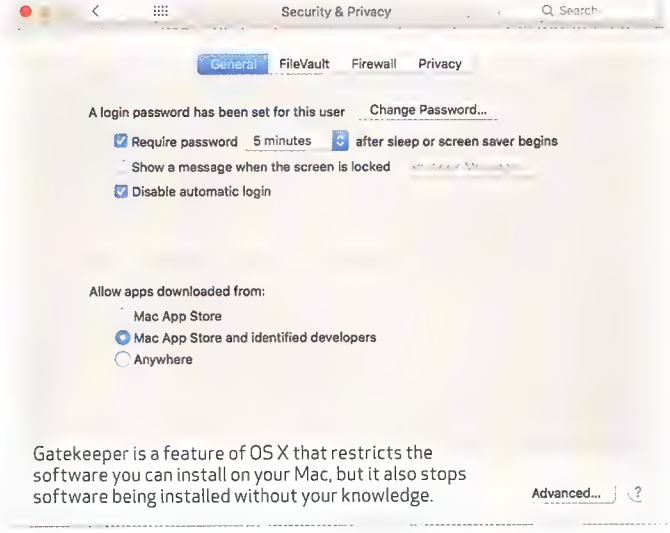
First, use the tools Apple gives you. Open up System Preferences and go to Security & Privacy. Tell Gatekeeper only to allow apps downloaded from the App Store or, at most, the App Store and identified developers. Activate FileVault — the performance hit is negligible, but anyone stealing your Mac can get nothing out of it. Switch on the Firewall — its default settings are good enough.

(Actually, under Firewall, click on Advanced … and activate Stealth Mode. This renders your Mac invisible to port sniffers.)

Finally, install Little Snitch to keep an eye on outgoing network traffic.


Security & Privacy
Block all incoming connections
Blocks all incoming connections except those required for basic Internet services, such as DHCP, Bonjour, and IPSec.
File Sharing (AFP, SMB)
Allow incoming connections
Screen Sharing
Allow incoming connections
Dropbox
Allow incoming connections
EPSON Scan
Allow incoming connections
fingerprintd
Block incoming connections
iTeleport Connect
Allow incoming connections
Automatically allow signed software to receive incoming connections
Allows software signed by a valid certificate authority to provide services accessed from the network.
Enable stealth mode
Don't respond to or acknowledge attempts to access this computer from the network by test applications using ICMP, such as Ping.
Cancel
OK
Advanced...

Stealth Mode stops your Mac responding to ping requests — hackers and bots won't even know it's there to attack.



Gatekeeper is a feature of OS X that restricts the software you can install on your Mac, but it also stops software being installed without your knowledge.

FREE | WWW.AVAST.COM/FREE-MAC-SECURITY

Avast Free Mac Security

Free, reliable detection.

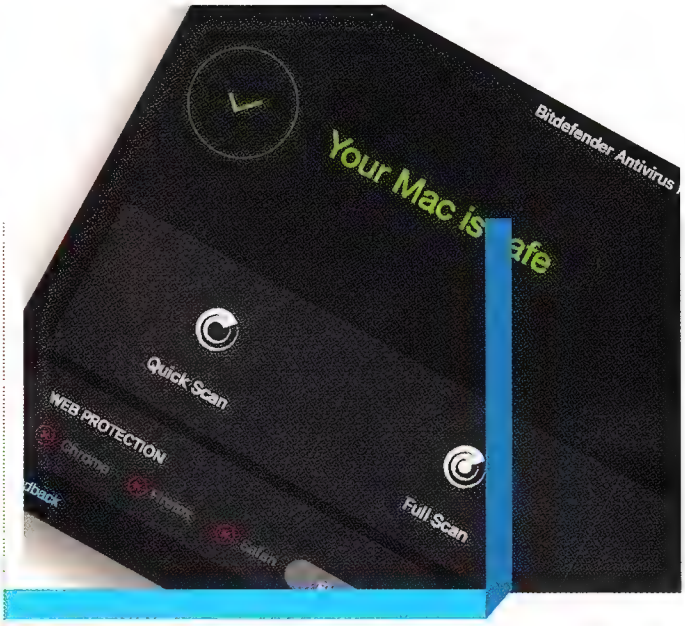
In tests conducted by av-test.org, Avast Mac Security not only managed to catch 100 per cent of the malware thrown at it, but did so with only a slight hit to system performance. That's impressive, considering the product is free. Avast provides three "shields": File Shield, Mail Shield and Web Shield. Each scans stuff coming into your Mac from whatever source and alerts you to any problems (the Web Shield requires you to download and install an extension for your preferred browser). You then have the option to move infected files to the "Virus Chest" for further action. In addition, Avast provides VPN products for desktops and mobile devices, which are also free.

And that's about it. As you might expect, given this is a free product, you don't get additional goodies such as a firewall or other protection. This is anti-virus, pure and simple. But it does it well and it does it free, and that's what it says on the metaphorical box.

Our one complaint is that the notifications Avast provides don't follow standard OS X interface guidelines. When a potential threat is discovered, you get a big orange splat thing in the shape of the Avast logo on the right of your screen, with no really obvious way to dismiss it (hint: click near the upper-left corner). Probably handy as an attention-getter, but irritating for taking up so much screen real estate (remember that Avast also looks for Windows malware, so chances are you'll get a lot of these alerts when you check your email).

Verdict

For a freeware package, Avast Mac Security is both powerful and lightweight.



$69.95 | WWW.BITDEFENDER.COM.AU

Bitdefender Antivirus for Mac

A spartan interface belies a powerful protector.

Long a champion of Mac anti-virus, Bitdefender managed to top AV Test's comparison of Mac AV tools with 100 per cent of nasties detected. And it did so with virtually no hit to performance – an important consideration, given many Mac users' reluctance to bother with security software at all. Optionally, you can add TrafficLight, a web browser extension (for Safari, Chrome or Firefox) that monitors pages you visit and jumps up to alert you to any suspicious behaviour such as phishing attacks or dodgy links on social media. It also spots web sites that track your browsing and report back – a handy feature for the privacy-conscious.

Unfortunately it's not free, and unlike other paid-for products, it doesn't come bundled with a whole lot of other tools for different forms of online protection. That's not necessarily a bad thing – what it does, it does very well and simplicity is a virtue. But when you look at the additional tools bundled with, for example, Norton, you may feel a little underwhelmed for value.

Note that there is a version of Bitdefender in the Mac App Store, but you shouldn't bother with that one. Limitations placed on developers by the Mac App Store basically make it incompatible with effective security software – you can't scan every file on a computer from within a sandbox.

Verdict

Reliable detection with minimal performance load, but with a smaller feature set than some.

ONE DEVICE, $59.95 PER YEAR; MULTI-DEVICE, MULTI-YEAR LICENSING ALSO AVAILABLE | BUYKASPERSKY.COM.AU

Kaspersky Internet Security for Mac

A solid AV tool, with additional goodies.

Kaspersky's Mac anti-virus, like most paid products, comes with a suite of other features such as a firewall, password management (essentially duplicating the role of the OS X Keychain) parental controls, web protection (automatically installing extensions for Safari, Chrome and Firefox) and "Safe Money" – a tool that specifically protects your financial information when shopping and banking online. Unfortunately, some features require a bit more manual fiddling than many unsophisticated users will be up for, so will end up unused.

Likewise the Parental Control feature, which at first looks pretty amazing, requires so much manual intervention that parents might not bother using it. To block your child from sending personal data, for instance, you have to activate Personal Data Control, and then specifically list the data (for example credit cards) your child is not meant to share. Surely this could be automated to some extent? It's a pity, because other aspects of Parental Control such as its interface for setting time limits are very nice indeed. Ultimately the best parental control is teaching your kids to be safe online.

Along with Avast, Norton and BitDefender, Kaspersky also managed to block 100 per cent of malware threats in AV Test's comparison, though it did so with a heavier performance load than Norton or BitDefender (and slightly lighter than the free Avast). We also liked the drag-and-drop interface Kaspersky provides for manually scanning a file – very Mac-like.

Verdict

Reliable malware blocking and a good feature set, but some features are a bit complicated.

ONE DEVICE, $59.99 PER YEAR; THREE DEVICES, $99.99; FIVE DEVICES, $129.99 | AU.NORTON.COM

Symantec Norton Security Premium

A suite with an avalanche of features.

Symantec has recently updated its Mac product, incorporating it into the Norton Security Premium suite, which provides security for up to five devices. As well as anti-virus, you get a very sophisticated firewall, web browsing protection (only for Safari and Firefox on Mac) and other goodies such as FileGuard, which password-protects individual files from prying eyes (although you can also do with OS X itself, so its value is neither here nor there really).

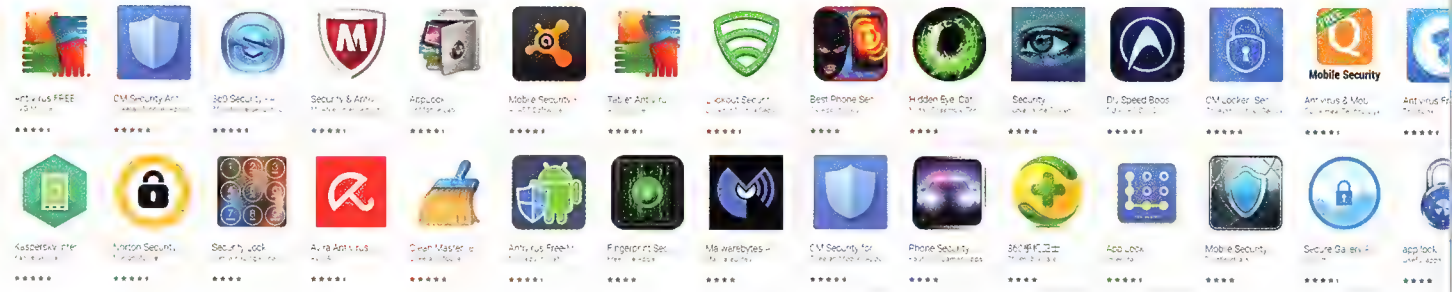
It's designed as a household product, so you get parental controls and other similar tools over and above what OS X (or whatever other OS you happen to have in your house) uses. If you have multiple devices protected it's handy to have one unified interface for monitoring and configuring all of that though. It's an extremely full feature set, but might seem a bit overwhelming if all you want is anti-virus.

The good news is that Norton Security for Mac blocked 100 per cent of the malware AV Test threw at it and had the smallest performance hit of all the products tested. Indeed, once you've paid for the product (a 30-day free version is available) Norton guarantees a refund if you ever do get infected. That's confidence.

It's worth mentioning that the firewall monitors both outgoing and incoming traffic, and can monitor based on applications as well as network ports. It's highly sophisticated but very Mac-like in its ease of configuration. In a lot of ways, it's more valuable than the anti-virus protection for which you're buying the product.

Verdict

Has a very full feature set, reliable protection and minimal performance hit.



Android has a huge array of free and paid apps that can help improve security.

Is Android security as dire as it seems?

Lindsay Handmer reveals critical info you need to know about protecting your Android smartphone or tablet.

In 2014, over 1.3 billion Android devices were sold around the world. That's a stupendously large number, so it's no surprise that the platform is seeing an increasingly large amount of attention from hackers and malware creators. Fortunately the latest versions of Android have plenty of security options built right in, and there are even more third party apps that let you totally customise your protection.

THE THREATS

Phones and tablets are an increasingly important portal into our digital lives, with access to everything from financial to personal information, which makes them a prime target for unscrupulous activity. Ultimately, attacks are designed to make money – be it simple spam and ads, to stolen credit cards, premium SMS scams, ransomware and even identify theft.

That said, it's still fairly hard to get malware on an Android phone. Self-replicating and spreading viruses (like on computer) don't really exist on Android. Instead, the biggest threat is from malicious apps, which a user has to agree to install. The problem is that apps are getting increasingly clever at tricking users into installing them, or posing as benign software. The lion's share of untrustworthy apps are found through the multitude of unofficial apps stores available online, so sticking to Google Play eliminates most of the problem.

SECURITY UPGRADES

The threat (however small) is still real, and in response, third party apps provide a huge range of security options, from malware protection to being able to remotely access and lock your phone. Google themselves are also constantly working on the problem – Google Play actually scans 200 million Android devices a day by default to check installed apps for security risks. The stats from these scans are promising: in 2014, less than 1% of devices had a potentially harmful app installed. For devices that only installed apps from Google Play, less than 0.15% had security issues. Over 2014, the amount of harmful apps installed actually dropped 50%.

PROBLEM AREAS

The open source nature of Android means Google can work with third party developers to quickly identify new malware and patch vulnerabilities. The downside is that even when Google releases updates, manufacturers can be slow to patch their custom versions of Android, and many older devices and unsupported will simply never get all security updates. In fact, it's estimated that only 20% of Android devices in use are still actively supported.

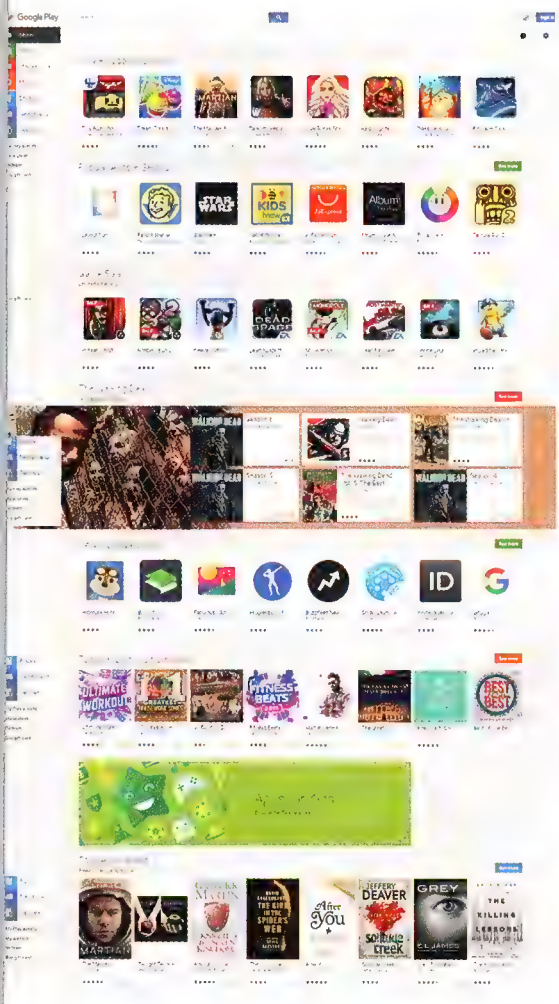
In Australia, grey import Android phones such as the Chinese OnePlus 2 are increasingly common, but some devices have actually arrived with malware and third party apps installed. It's not just a case of doing a factory reset either – the problem software is a default app and not removable without flashing to a whole new ROM.

YOUR SECURITY

With a bit of common sense and Android's inbuilt security, it's entirely possible to avoid malware, and keep your phone safe if you lose it. Security apps are still worth a look though, and can give an extra layer of protection, whilst providing a richer set of features to help customise your experience.

LABS RESULTS: ANDROID SECURITY APPS

	INDUSTRY AVERAGE	AVG ANTIVIRUS FREE	AVAST MOBILE SECURITY	AVIRA FREE ANDROID SECURITY	BITDEFENDER MOBILE SECURITY AND ANTIVIRUS	BULLGUARD MOBILE SECURITY AND ANTIVIRUS	ESET MOBILE SECURITY AND ANTIVIRUS	KASPERSKY INTERNET SECURITY	MCAFEE SECURITY AND ANTIVIRUS	NORTON SECURITY AND ANTIVIRUS
MALWARE DETECTION	99.30%	99.20%	99.70%	100%	100%	98.50%	100%	99.90%	98.50%	99.90%
PROTECTION SCORE		5.5/6	5.5/6	6/6	6/6	5.5/6	6/6	6/6	5/6	6/6
USABILITY SCORE		6/6	5.5/6	5.5/6	6/6	6/6	6/6	6/6	6/6	6/6



Fewer than 0.15% of users who only use Google Play have security issues from apps.

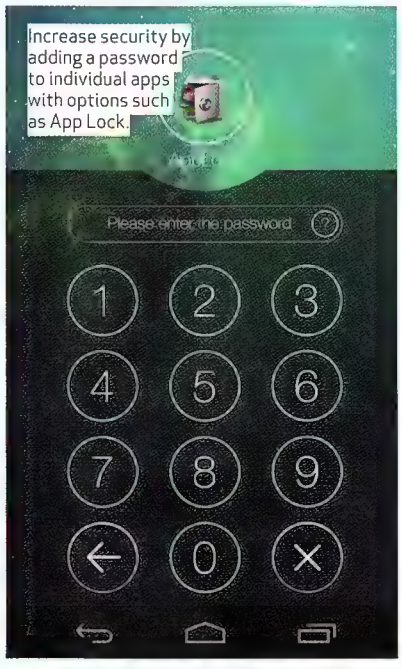
Labs results: Android Security Apps

All testing results were compiled from AV-Test. The independent German IT security institute runs comprehensive tests using 3,336 malware samples on the latest versions of security apps. Note that the usability score in the table is compiled from performance and battery life impacts, as well as any false positives recorded.

SOPHOS FREE ANTI-VIRUS AND SECURITY	TREND MICRO MOBILE SECURITY & ANTIVIRUS	WEBROOT SECURITY
100%	99.80%	99.40%
6/6	6/6	5.5/6
5/6	6/6	6/6

10 things you can do to secure your Android

By default, Android is pretty secure, but there are a whole host of extra options you can turn on or add with third party apps. Here are our top ten tips to get you started down the path to a more secure Android experience.



1 GET TO KNOW YOUR DEVICE
Spend some time exploring the quite powerful security options available in stock Android and make sure they are fully set up. Test your security features such as remote tracking before you need them. Make sure you download the latest updates. For devices that get shared, set up multiple user accounts.

2 LOCK IT DOWN
Android already lets you apply a pin code, use face recognition or (on compatible models) unlock via fingerprint. You can also disable locks with trusted locations, Bluetooth devices, NFC tags or even on body detection that learns the patterns of how you move and locks the phone when not in use.

3 ENCRYPT YOUR PHONE
Even after doing a factory reset, some data can be recovered. New Nexus devices encrypt by default, but it can be in Android 4.1 or newer. Encryption is also available through third party apps for specific folders rather than the entire phone. Encryption can create a small performance loss.

4 TURN ON DEVICE TRACKING
Installed by default, Android Device Manager lets you ring, track, lock and erase your phone via the internet. Check you have it linked to your Gmail account and make sure you frequently backup your info so you can wipe your phone without worry about data loss. Third party tracker apps give extra features, such as the ability to take photos remotely.

5 MANAGE YOUR PASSWORDS
Weak passwords are often easier to type on a phone, but can give easy access to your accounts. Use two factor authentication where possible on your Google account and sensitive apps. Don't save passwords by default. Apps such as LastPass can help manage passwords for those who are forgetful.

6 LOCK ACCESS TO APPS
Add an extra layer of security (or avoid an unlock pin) by locking individual apps. Banking, email, photos or messaging all contain sensitive information. Protect your data by adding a pin code to open them. This is also useful for devices that need to be shared.

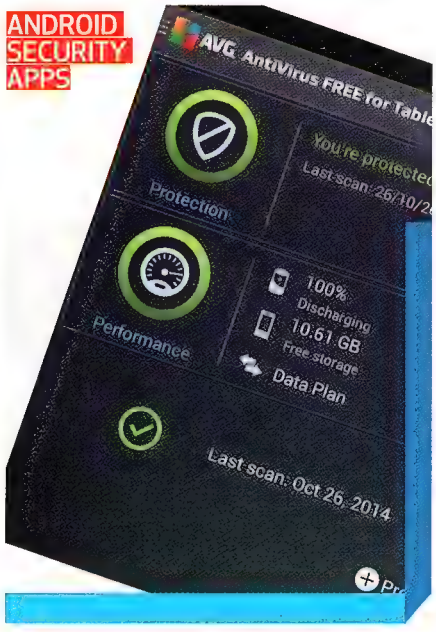
7 USE A VPN
Increase your online security and privacy by routing all your data through an encrypted channel. A VPN can also get around geoblocks or local firewalls. Avoid public Wi-Fi without a VPN, as it's very easy for your data to be hijacked and recorded.

8 USE MORE SECURITY APPS
Going beyond just virus and malware protection, you can also install apps that block ads, give you better remote control over your phone, or allow you to send encrypted emails and texts. Or install the Orbot app for secure communications via the Tor network.

9 AVOID UNOFFICIAL APPS
It should go without saying, but stick to apps approved by Google. In addition, always read what permissions apps are asking for, or check them with an app such Permission Watchdog. Avoid rooting your phone, as it can make it easier for malware to gain access.

10 LOCK SCREEN CUSTOMISATION
Review and customise your lock screen notifications, as sensitive information such as two factor authentication codes could be displayed even when locked. Consider adding contact details such as email to the lock screen so your device can be returned if lost.

ANDROID SECURITY APPS



$14.90 PER YEAR | WWW.AVG.COM

AVG Antivirus

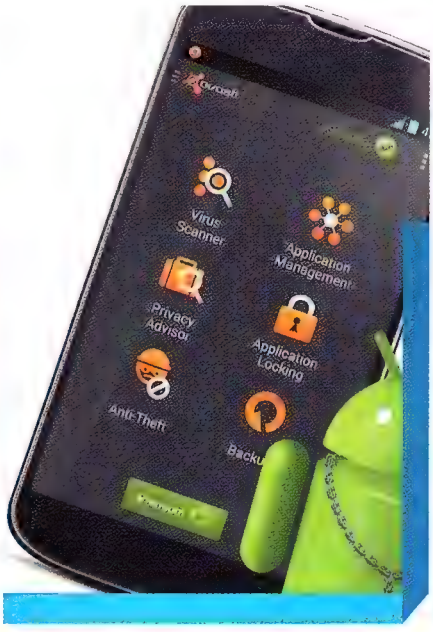
The Android AV suite with over 100 million installs.

AVG provides automatic scanning of apps and files, as well a real time protection when surfing the net. It also has a built in task killer – but that's a feature that you shouldn't really use or need. AVG is supported by ads, but there is an ad free pro version available for $14.90 on the Google Play store as a one-time payment. But when you install the app it instead offers the Pro version as a $14.90 yearly subscription (or $3.90 a month) without making any potential difference clear. Pro features include a camera trap that records anyone trying to access your device. It also lets you add coded access to specific apps and will automatically lock down your phone if the sim card is replaced. It can also backup apps to an SD card. The app is well laid out, but somewhat laggy to use. AVG manages to pick up 99.2% of the latest Android Malware, which is actually slightly below the industry 99.3% average.

Verdict

Odd pricing and slight lag means give AVG a miss.

★★★☆☆



$19.99 PER YEAR | WWW.AVAST.COM

Avast Mobile Security and Antivirus

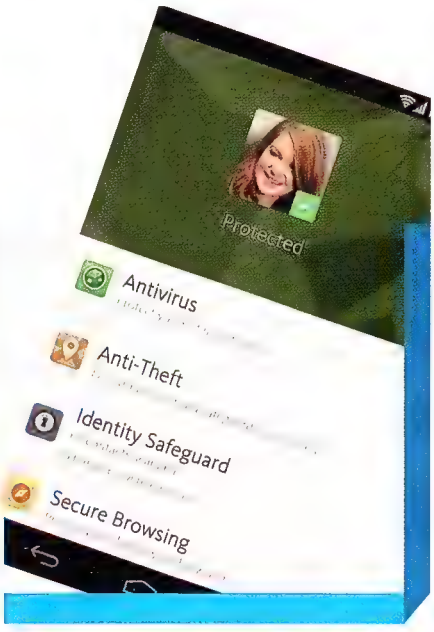
A simple yet powerful option.

The free version automatically scans for malware, but also includes heaps of features such as app permission monitor, text and call filter, Wi-Fi scanning, network data metering, a firewall and the ability to individually lock two apps. Getting up and running is very painless, though annoyingly for us the app immediately reported one problem, but did not say what the problem was or give any more info. While it can be controlled through the one app, some functionality needs separate Avast apps to be installed, such as anti-theft. Avast has a premium version which includes extra features such as the ability to individually lock as many apps as you want, ad detection, geofencing, remote data recovery and remote identification. Instead of an annual sub you can pay $2.49 per month. You can try free for 30 days by inviting 5 friends to install the app. Notable missing features include parental controls and backups management. Avast picks up 99.7% of malware.

Verdict

Solid features, but a little more expensive than some of the competition.

★★★½☆



$9.02 PER YEAR | WWW.AVIRA.COM

Avira Free Android Security

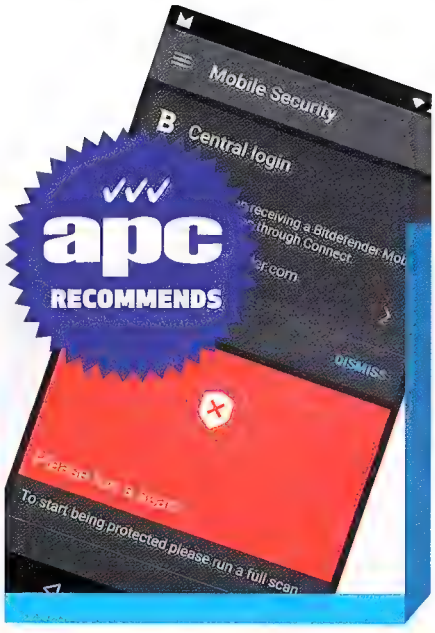
Top-notch protection for your mobile.

Avira handles the typical scanning for malware and rogue apps, but will also track a stolen phone, and remotely lock or wipe it. You can also trigger a loud siren or send details to prompt whoever found it to return it to you. Avira also lets you lock down individual apps with a code. The handy (and unique) Identity Safeguard feature sends a notification when a company where you have an account is hacked. Avira has a premium version available as in-app purchase. You don't get a lot for your $9.02 – safe online browsing protection, more frequent updates and access to premium support. Impressively, Avira picked up 100% of the latest Android malware and is also light on resources so shouldn't slow down your device. While Avira doesn't have as many features as some of its competition (but includes free app locking, which makes the premium upgrade less desirable) it does give an excellent extra layer of malware protection for free.

Verdict

While the free version is great, the paid upgrade isn't really worth it.

★★★½☆



$14.95 PER YEAR | WWW.BITDEFENDER.COM

Bitdefender Mobile Security and Antivirus

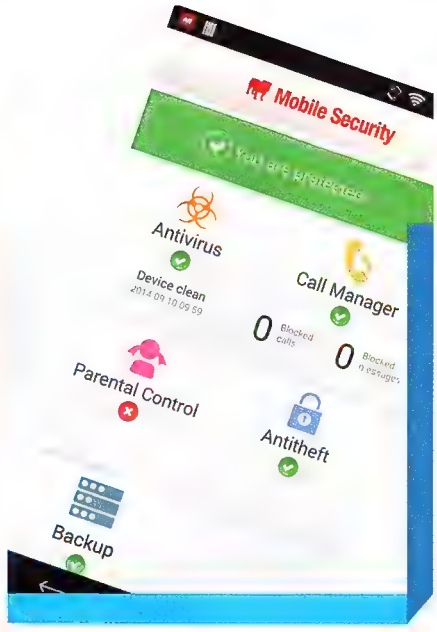
Feature-packed but no free version.

Bitdefender only has a paid version, with a 14 day free trial that starts immediately. After that the app will cost $14.95 a year or $1.49 a month. Aside from malware protection, the app includes an anti-theft tracking system, privacy settings advisor, safe browsing protection and can add a password lock to your individual apps. It can also extend protection to your smartwatch, and sound an alert if you are separated from your phone. The app requires you to create an account (or sign in with your Google one) before you can start scanning. The main dashboard is deceptively simple but the menu system uncovers the full array of options. You do need to spend some time setting up Bitdefender, and it requires more of a hands-on user to get the most out of it. On the plus side, it is well laid out and very responsive, even when scanning. Impressively, Bitdefender managed a 100% detection rate on malware and offers excellent protection.

Verdict

One of the better paid security apps available.

★★★★☆



$24.95 PER YEAR | WWW.BULLGUARD.COM

Bullguard Mobile Security and Antivirus

Provides protection across multiple devices.

Bullguard doesn't have a free version, instead offering a paid app with a free two week trial. It costs $24.95 a year but can be installed on up to three devices. If purchased at the same time, a second year's protection costs $15. It offers the usual antivirus and antitheft, as well a one click backup solution. You also get a call filter and parental controls, but no web protection. You can also control all the app settings through an online portal, which is lucky, as the Bullguard app seems a lot less polished than some of the competition. After installing, it needs an account created and there are no quick login options. You can't pay for a subscription through the app either - it has to be done via the website (which lists two prices), then a code manually entered. Bullguard managed a 98.5% detection of malware, which is actually below the 99.3% industry average. While the apps large feature set makes it worth a look, ultimately the high price and clunky interface let it down.

Verdict

Not enough features and too many niggles to be worth it.

★★★☆☆

FROM $14.95 PER YEAR | WWW.ESET.COM

ESET Mobile Security and Antivirus

Full-featured and affordable.

While free protection is pretty basic, including malware scanning and anti-theft, the premium features excel. You get a more robust anti-theft setup with photo taking, online device management, scheduled scanning, safe online browsing and active device settings monitoring. ESET will also audit your app permissions, let you block calls and messages, set on charger-only scans and even view mobile security help videos. The ESET premium upgrade option is free for 30 days, then has a range of pricing that starts with a basic $14.95 for one device for one year. Bumping it up to two years costs $22.43, whilst three is $31.39. You can also add protection for extra devices – starting at $5 each and getting cheaper the more you add. ESET is easy to navigate and use, and perhaps more importantly, picked up 100% of malware in tests. It's a shame the feature set does not include a few more options, such as app locking, which would make it perfect.

Verdict

A great all round option with an affordable pricing structure.

★★★★☆

$14.95 A YEAR
WWW.BUYKASPERSKY.COM.AU

Kaspersky Internet Security

Simple and easy to use.

The core Kaspersky malware and antivirus protection is free, along with call and text filtering and a decent anti-theft solution that includes mugshot capture. Upgrading to premium will cost $14.95 a year per device. The premium version is available as a free 30 day trial by default, with an in-app purchase to upgrade. Extra functionality includes real time scanning, online browsing protection and automatic detection of phishing texts. You also get privacy protection, which can be set to hide selected contacts from other users of your device. Kaspersky detects 99.9% of malware, but lacks a few useful features compared to the competition. Notable omissions include app locking and backup managements, as well as the less common parental controls. On the plus side, the app is easy to set up and navigate and can be managed through an online portal. It's also low impact on your devices resources which helps maintain battery life.

Verdict

The paid upgrade isn't really worth the money compared to what you get with the free app.

$29.95 A YEAR | WWW.MCAFEE.COM

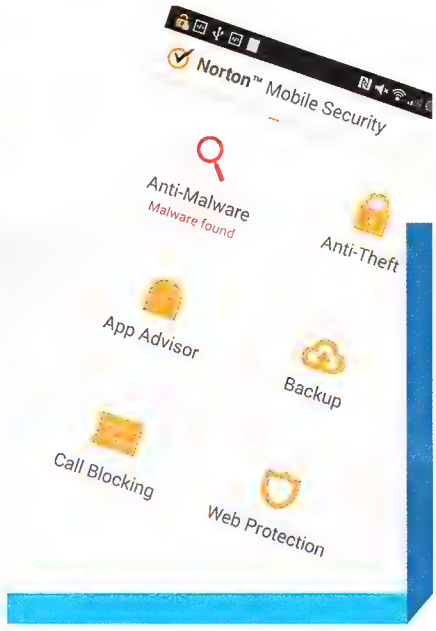
McAfee Security and Antivirus

A comprehensive free option?

Unlike other security apps that have quite pronounced free and paid tiers, McAfee offers almost everything for free. The catch is an ad supported environment – albeit a fairly unobtrusive one. A hefty $29.95 a year let users ditch the ads, as well as get phone support and media backups. The free features include comprehensive anti-theft that allows the usual track/lock/wipe as well records pictures. McAfee has also included great privacy controls, with multi user app profiles, app locks, an app permission checker and a call and SMS filter. The app has inbuilt performance and battery optimisation options and can help clean up your storage to create extra space. It will also give real time online protection and help make unsecured Wi-Fi safer. The McAfee setup and options can be a little tricky to navigate, but generally it's easy and fast to use. It is slightly behind when it comes to protection though, finding 98.5% of the latest Android Malware.

Verdict

Unless you really hate ads, the free version is an excellent option.



$29.99 A YEAR
WWW.MOBILESECURITY.NORTON.COM

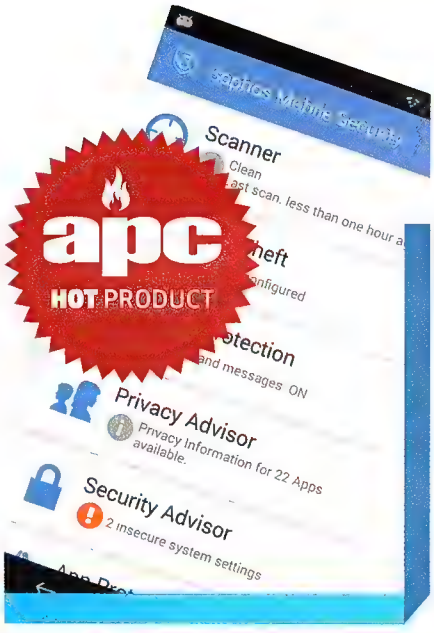
Norton Mobile Security

Does the mobile version of this big-name suite hold up?

Unlike the computer version that is fairly universally disliked, the mobile version of Norton has a 4.4 (out of 5) star rating on Google Play from over half a million users. The package is pretty normal – it offers malware and virus scanning, online protection, anti-theft options and lets users filter calls and messages. You can also backup contacts and share them across devices, including to iOS. The app comes with a 30 day trial, after which the premium version of Norton will set you back $29.99 a year, or for two years, $49.99. There is still a very basic level of free protection provided, such as malware scanning, if you don't upgrade. The actual installation and setup experience was quite painless, and the app is well laid out and easy to navigate. We experienced some lag issues at first, but they went away after the app got settled. Protection is good, and Norton picks up 99.9% of Android Malware in tests. Ultimately though it's pricey considering the feature set.

Verdict

Not inherently bad, but not great value either.



FREE | WWW.SOPHOS.COM

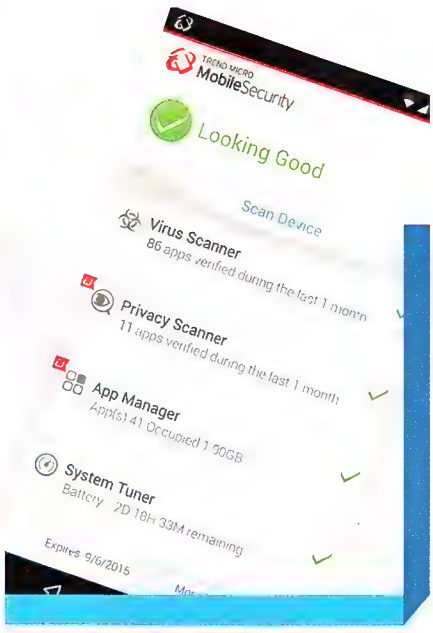
Sophos Free Antivirus and Security

Totally free, with no catches.

While other companies were spending time dividing free and paid options, Sophos just concentrated on building the best security app possible. Then didn't charge for it or include ads for personal use – instead making money from commercial applications. Sophos has a solid feature set – the only key functionality missing is an app locker. It includes the malware scanning, real time web protection that will provide warnings about suspect websites and block phishing attacks via emails and SMS. It can track, lock, wipe and message a missing phone, but doesn't allow pictures to be taken. The Sophos app also includes a call and text filter, parental controls and a security adviser that can warn about app permissions. And in tests, the app picked up 100% of Android malware. The only glitch was identifying two legitimate apps from third party app stores as potential threats. This is one of the better Android security apps available, and free to boot.

Verdict

Easily our top choice and better than most of the paid apps.



$29.95 A YEAR | WWW.TRENDMICRO.COM.AU

Trend Micro Mobile Security & Antivirus

All-round protection: is it worth the price?

The free version of the Trend Micro app includes a 30 day trial of the premium features, after which it costs $29.95 a year. Without coughing up any cash, users get antivirus protection, billing security, 50MB of cloud storage for backup of contacts, a battery saver and memory booster, history cleaner and a Facebook privacy scanner. Going pro lets you block Malware laden apps before they can be downloaded and scans all your apps for privacy issues. It also enables lost device protection, which lets you do the usual array of tracking, locking and wiping a missing device. The Trend Micro app has included safe surfing parental controls as well as call and text filtering. The auto Just-a-Phone feature shuts down non-essential background processes when the battery is low to eke out a little more life. You also get an app manager, to see where all that free space has disappeared to and make it easy to clean. Importantly, the app picks up 99.8% of Android malware.

Verdict

Does provide some unique features... if you can stomach the high price.

$4.99 A YEAR | WWW.WEBROOT.COM

Webroot Security

Is it worth going for a cheaper option?

With both a paid and free version, Webroot makes it easy to customise your security level. The Webroot Security Premier app costs $4.99 a year, the PC suite includes the mobile version in its price. In the free version, you get automatic malware and virus scanning and continuous ongoing protection. The app will also warn about phishing attacks and block unsafe websites. It has call and text filtering as well as extra social media protection. The anti-theft options include the ability to track and remotely lock your device, but not wipe it, which is only possible with the paid app. Other paid features include an automatic locking system if the SIM is removed as well as battery and network monitoring. It can also identify apps that have potentially invasive permissions, or ones that could cost you money, track your location or drain your battery. Webroot picks up 99.4% of malware – a touch better than the 99.3% average.

Verdict

Cheaper than most paid options, with a good array of features.

THE
MOST FUN
YOU CAN
HAVE WITH
YOUR HANDS
WITHOUT
GOING
OUTSIDE.

games radar
MORE KICKS PER CLICK

Security on iPhone & iPad

Apple's mobile devices are some of the more secure devices, but they're not impervious to attack. Matthew JC. Powell reveals what you need to know to protect yourself.

Security was at the heart of Apple's design process for iOS, at least partly because of frustration with security issues in desktop operating systems including its own. This is why you can't install software from anywhere but Apple's App Store onto an iOS device, and it's why you have precious little ability to customise iOS devices. It's a "walled garden" – but a secure one.

The exception has been "jailbroken" devices – those that have been modified to allow users to install software from other sources and to customise their iOS experience in other ways. If you choose to compromise your device's security, you should understand the risks.

In the past year or so, there have been malware attacks that could affect iOS devices regardless of whether or not they were jailbroken. One, called Masque Attack, attacked companies that allow their users to install iOS software from enterprise servers. Once the server was compromised, malware replaced seemingly legitimate apps on users' devices.

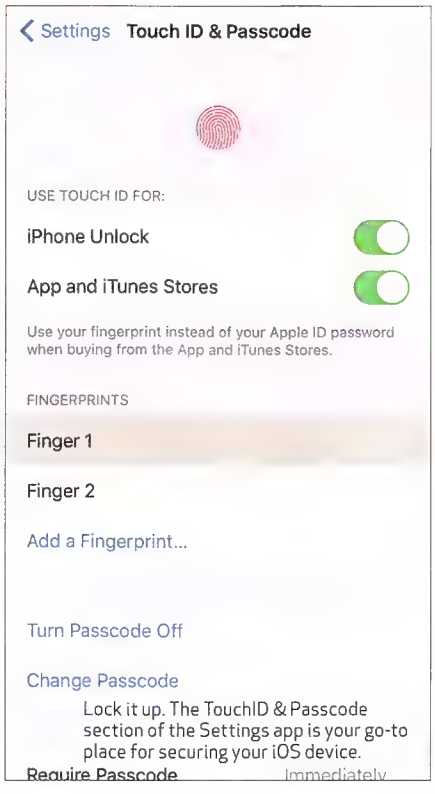
The other, WireLurker, modified iOS apps in users' iTunes libraries on their Windows computers. When the user plugged their iOS device into the computer, the modified apps would be installed.

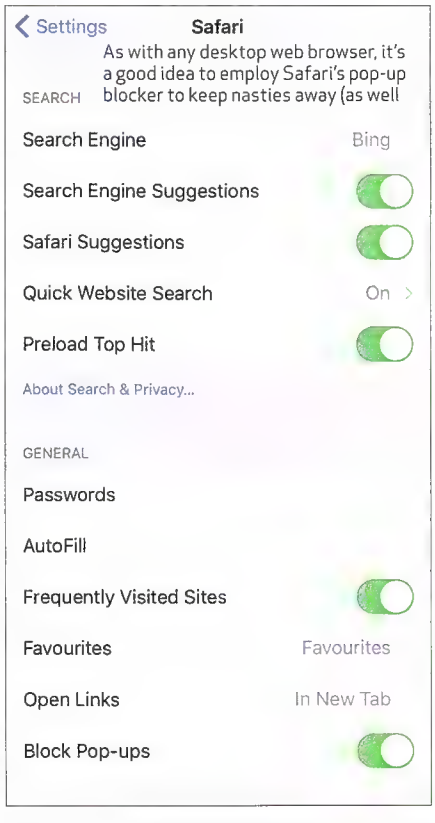
Finally, there was the Great App Store Hack, which appeared at first blush to render all of Apple's claims about iOS security moot. Apps which users had legitimately downloaded directly from the App Store had been infected with malware called XcodeGhost.

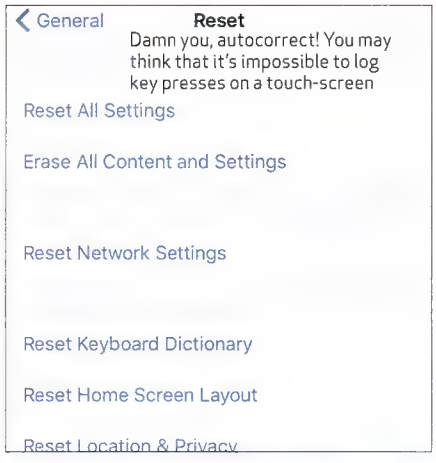
In fact, the App Store hadn't been hacked. The malware's authors targeted a number of developers (primarily in China) with a modified version of Apple's Xcode development environment. When these trusted developers updated their apps, they unwittingly uploaded infected code to the App Store.

In all three cases, Apple responded swiftly by stopping the affected apps from launching, and it says it has put processes in place to head off similar attacks in future.

The bottom line is that iOS remains a secure platform, but its users must be vigilant.


Settings
Touch ID & Passcode
USE TOUCH ID FOR:
iPhone Unlock
App and iTunes Stores
Use your fingerprint instead of your Apple ID password when buying from the App and iTunes Stores.
FINGERPRINTS
Finger 1
Finger 2
Add a Fingerprint...
Turn Passcode Off
Change Passcode
Lock it up. The TouchID & Passcode section of the Settings app is your go-to place for securing your iOS device.
Require Passcode
Immediately




General
Reset
Damn you, autocorrect! You may think that it's impossible to log key presses on a touch-screen
Reset All Settings
Erase All Content and Settings
Reset Network Settings
Reset Keyboard Dictionary
Reset Home Screen Layout
Reset Location & Privacy

Make your iOS device more secure

The primary way baddies can attack your iPhone or iPad is by getting their hands on it. If you're not using a passcode on your device (so the kids can play with it, for example), you're at risk of your data getting into the wrong hands.

Open the Settings app and tap on Touch ID & Passcode. Then tap Turn Passcode On. You'll then have three options: a custom alphanumeric code, a custom numeric code, or a custom 4-digit numeric code. Your best option is a custom alphanumeric code — string some random words together and teach them to your kids. It's easy to remember "banana2monkey" but almost impossible for someone else to guess.

Also in the Touch ID & Passcode section, you can disable certain functions of your device that can be accessed without unlocking — such as voice dialing, Notifications View and Siri.

You should also enable Erase Data, which will wipe the device after ten incorrect passcode attempts. (Teach your children well!)

Finally, always make sure you install the latest software updates from Apple. As well as bug fixes and new features, they dress security vulnerabilities when they arise.

Oh yeah — don't jailbreak. ■

Smarter passwords made easy

Weak passwords are one of the biggest risks to your online security. Joel Burgess tests nine password managers to find out which offer the best mix of usability and security.

Every time you re-use the same password for a different internet account, you dramatically increase the likelihood of your online security becoming compromised. According to US security company DigiCert, 73% of people use passwords multiple times and the average password is only six lower-case characters long – meaning an expert hacker could crack it in under 3 minutes. Not only are the vast majority of passwords easy to crack, but the companies storing your login details often aren't as safe as you might think they'd be.

A visualisation of the world's biggest data breaches (tinyurl.com/APC422-Hacks) shows just how many big-name companies have been hacked – and it's worth checking out the above link, as it may reveal that one of those hacked companies had important passwords of yours, passwords that could now be roaming around the internet. As you can see, it isn't just social media companies that have been compromised, the trail of destruction goes all the way up to the US's biggest bank and the government of Greece.

That said, if the idea of remembering unique passwords for everything hurts your head, you're not alone. Thankfully password managers can transfer the burden of generating and storing strong (ie. gibberish!) passwords onto your computer. Don't be misled, switching to a password manager may not be a rapid process initially, but once you're using the system it's dead simple – and it will be a lot easier than attempting to recover money stolen from a hacked bank account.

WHAT ARE PASSWORD MANAGERS?

Password managers are systems that collect all the passwords you use in one place, allowing you to store secure, randomly-generated strings that can then be used to easily unlock your online accounts. Many browsers have the ability to save passwords, but this only offers limited security – and in fact, most security experts warn against letting your browser remember passwords (tinyurl.com/tla37-brow). The other saving grace of password managers is that they can check the SSL certificates of sites, so you don't enter your password into a fake 'phishing' web site that is imitating something legitimate like Facebook.

The best password managers encrypt your data using a master password. This means you only have to remember one password to access your entire password library. As you've only got that one password, however, it's critical to make it one that's strong and therefore difficult to crack. Preferably, it should be an eight-character (or longer) combination of numbers, upper-case letters, lower-case letters and symbols. Other than that, an email address, mobile phone and a bit of patience are all it takes to be secure online.

Choosing a password manager

These are the key elements to consider when picking a password manager.

COMPATIBILITY

Most are compatible with Mac and Windows OSs and plug into the major four web browsers (Internet Explorer, Chrome, Safari and Firefox), but smartphone and tablet support varies considerably.

APP OR PLUGIN?

Password managers generally come in two forms: direct browser plugins with online accounts, or standalone applications. The plugins tend to have more cloud integration, while standalone apps have the added security option of not syncing online.

TWO-FACTOR AUTHENTICATION

Some have no integration with this extra security measure, some have their own service and the best offer linking with independent two-factor authentication services.

DIGITAL WALLET/INFO STORAGE

The option to auto fill forms such as name and address or credit card details from a secure place can make it much faster and safer to purchase things on the internet.

PRICE

Just because a service is more expensive or charges a subscription fee doesn't necessarily mean it's any more secure or easy to use.

IMPORT OPTIONS

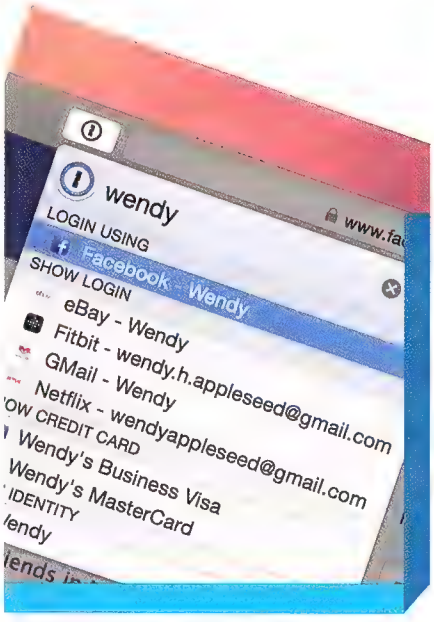
Some password managers can capture any password you've ever saved (in a web browser or otherwise) easily, while others have trouble importing them — even from other password managers. Keep an eye on this feature if you're already using an existing password manager.

COMMUNAL PASSWORDS

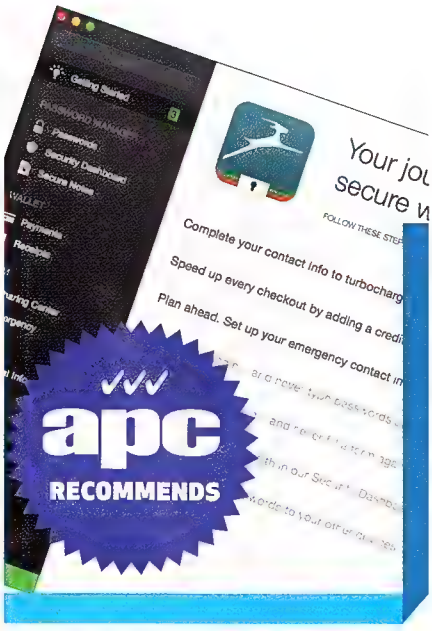
You may want to let someone else have a specific password and rather than letting it loose in an email, some password managers will let you share encrypted passwords with other account holders using the same platform.

AUDITS & HACK ALERTS

A number of apps will be able to tell you how secure each of your passwords are and give you an overall security score. The best apps also keep a log of companies that are hacked and will notify you if you have an account with them.



DESKTOP APP SINGLE LICENCE, $46.99; ANDROID AND IOS APPS FREE | AGILEBITS.COM/ONEPASSWORD



FREE WITHOUT SYNCING, SHARING, WEB ACCESS OR BACKUP; PREMIUM SUBSCRIPTION US$39.99 PER YEAR | DASHLANE.COM

FREE | KEEPASS.INFO

1Password

Good on security, bad on privacy.

There are advantages to 1Password's stand-alone, application-based approach, and the service also offers browser plugins (and a unique widget), but overall, we found it a little less useful than some others here. Why? Well, firstly it isn't quite as versatile, focusing only on the most common Mac, Windows, iOS and Android operating systems. Unfortunately the 1Password app can only import passwords from a couple of sources and because it needs you to find the saved 'password bank' files for these, which is more difficult than it needs to be. Recently, a Microsoft engineer discovered that websites you visit are indexed without encryption when using the 1Password Anywhere feature, and while this doesn't compromise your passwords or account details, it does make it easy for a hacker to know what secure sites you visit and have passwords for – a little concerning, considering you're trusting them with your passwords.

Verdict

A little more bland than some, but you can buy it outright.

★★★½☆

Dashlane

Would be a great option... if it dashed the price.

This desktop application has one of the most attractive UIs and packs an extensive features list. However, it's also one of the most expensive, and the handful of benefits it offers over LastPass arguably don't add up to the subscription price. Dashlane can import from a wide variety of locations and has a simple, engaging tutorial to start you off. It'll also walk you through all the more in-depth features of the service and gives a full security report of the compiled passwords. Like LastPass, it keeps track of big hacks and automatically advises you when you should change your password. Dashlane outstrips LastPass in two ways; it has even more versatility in two-factor authentication options and it can automate the process of changing passwords after hacks. Dashlane isn't as good as LastPass at recognising web boxes on more obscure sites, but it doesn't have any major technical downsides. The only drawback is the price.

Verdict

The most comprehensive and user friendly password manager available, if you have the dosh.

★★★★☆

KeePass

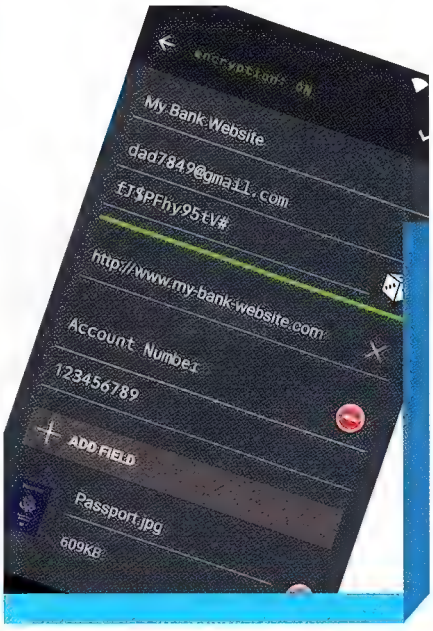
A secure and versatile DIY manager.

KeePass is a free, open source program that's designed to run on Windows, but is also compatible with Linux and Mac via official ports. It doesn't have any bells and whistles, but it uses the Advanced Encryption Standard (AES) – approved by the NSA for top secret information. If you want access to your passwords remotely or on a mobile device, you'll need to copy the encrypted file-vault manually using a cloud storage service like Dropbox or Google Drive. KeePass can import passwords from a large list of other password managers and offers the ability to customise or change everything about it, right down to using either a master password, a file-based encryption key or both. If you're a stickler for customisability, have a background knowledge of software and don't mind plugging in extra hours to get the exact system you want, then KeePass is for you. If not, any of the other password managers would be a better fit.

Verdict

A free open source password manager that is great if you put in a bit of work.

★★★★☆



SINGLE-DEVICE SUBSCRIPTION, US$9.99 PER YEAR; MULTI-DEVICE SUBSCRIPTION, US$29.99 | KEEPERSECURITY.COM

Keeper Security

Definitely not a keeper.

Though it offers a free 30-day trial, Keeper will regularly prompt you to upgrade during that time – delivering frequent threatens that without the upgrade's cloud-encryption, you'll be unprotected. As with some of the other less full-featured password managers here, Keeper only allows you to import existing passwords from files, making it hard to migrate from a cloud-based service and there's no audits on password security, or alerts if one of the sites you use has been hacked. Annoyingly, the app automatically signs out every time you switch to an internet window, which strikes the wrong balance between security and usability. The password generator is tucked away in the vault editing section, making it a pain to find and use. At US$9.99 per year on one device (or US$29.99 for multiple devices) it costs more on average than the leading apps. Keeper isn't a bad package, but it wouldn't be first on our list.

Verdict

More concerned with pushing you into a paid subscription than offering a top shelf product.

★★★☆☆

FREE; PREMIUM, US$12 PER YEAR
LASTPASS.COM

LastPass

The last password you'll ever need.

LastPass is one of the most feature-packed of the password managers and is also the most broadly-compatible, with apps and browser extensions for almost every major platform. LastPass can import password lists from over 30 sources and while using it on a single desktop is free, if you want cloud access or smartphone apps, you'll need to pay the yearly subscription. LastPass offers some neat features, like security reports on the number of duplicate passwords you have and the total number of secure passwords stored in your vault. It's also compatible with a number of two-factor authentication services. It's one of the only services that keeps track of major data breaches and will cross-reference the websites you have stored in your vault, informing you if an account has been compromised. LastPass was recently acquired by online B2B software company LogMeIn, so we're hoping the new owner keeps up the legacy of this gem.

Verdict

Sophisticated password management that won't break the bank.

★★★★½

WINDOWS AND MAC APPS US$19.99 PER YEAR; ANDROID, IOS AND WINDOWS PHONE APPS ALL US$9.99
MSEVENSOFTWARE.COM

mSecure

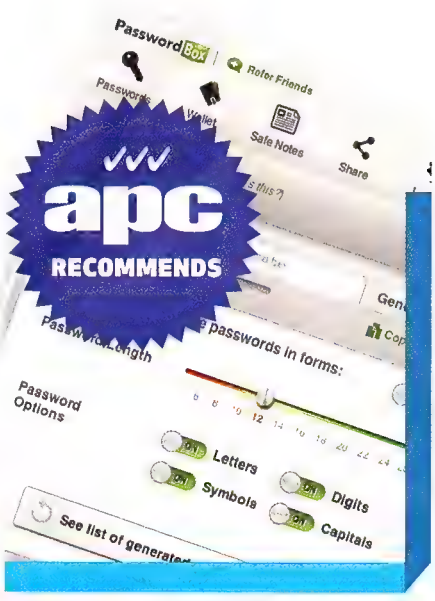
Mediocre, miss, minus? What could the M stand for? For us, it's 'meh'.

mSecure is a half-decent application, with an inoffensive layout and features that cover all the basics, but it's confined in the same ways seen in other file-based password managers. Importing is difficult and you can only sync your password file by logging into a Dropbox or iCloud account, which makes this harder than it should be. The desktop apps for Windows and Mac are US$19.95, and for Android or iOS it's US$9.99. However, unlike most others there are no browser-extension options – though you can manually link account logins to URLs in the editor. It will only generate passwords from within editing pages and the lack of a widget or browser shortcuts makes the process a little cumbersome. It will automatically copy a password to the clipboard when you click through to a site stored on file, but by comparison this isn't all that helpful. mSecure is usable, but it feels tired compared to others we reviewed. There's nothing here that really gives it an edge.

Verdict

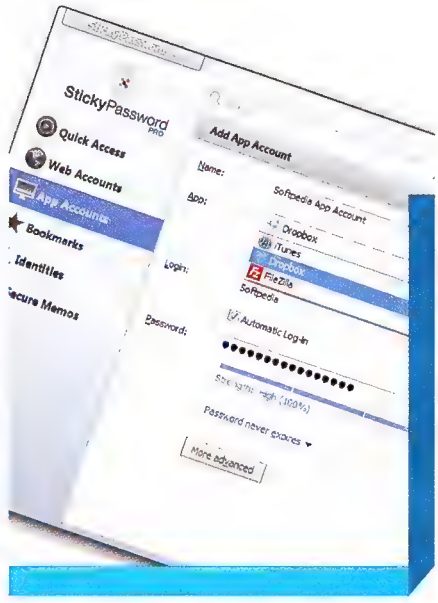
You can do better at this price.

★★★☆☆



FREE (UNTIL MID 2016) | PASSWORDBOX.COM

US$19.95 PER YEAR | ROBOFORM.COM



PREMIUM SUBSCRIPTION, US$19.99 PER YEAR; ANDROID AND IOS APPS FREE | STICKYPASSWORD.COM

PasswordBox

A solid free offering that is about to become history.

This browser extension is super easy to use and since it was acquired by Intel Security late last year, the premium service has been available for free. However, that acquisition also means PasswordBox has a finite lifespan, with support ending sometime in 2016. PasswordBox has no stand-alone application, so it focuses instead on delivering as many features as it can directly in your browser. Your passwords are stored in the company's encrypted cloud and can be easily synced to apps on iOS and Android. A convenient password generator, form-filling features (and with the promise of two-factor authentication and fingerprint security on the way) all add up to make PasswordBox a well-rounded option. We wouldn't be too deterred by the lack of future support, as most of the better password managers make importing passwords simple, so you can use PasswordBox for free before you swap over to another one.

Verdict

Amazing free software that's soon to be extinct, but easy to swap out of when it all ends.

★★★★☆

Roboform

Robo-yawn.

Roboform is another application-based password manager that has extensions for all the major web browsers. Smartphone apps for Android, iOS and Windows Phone are all available for free and it has a personalised webpage that'll let you quickly log into your most used sites. Instead of retroactively capturing personal info when you fill in a webpage, RoboForm asks you to create a profile page in your safe that has all your details. It's not a bad idea, but many other password managers, and even browsers themselves, can automatically grab this info. The cloud-based version costs a reasonable US$20 per year, allowing you access from anywhere via a web-based interface and unlimited desktop licences for the application. But seeing as you can only import passwords as CVS documents, it doesn't offer third-party two-factor authentication, and you can't see if services have been hacked (or auto-replace passwords that have).

Verdict

A decent but bog standard password manager, that's straight off the production line.

★★★½☆

Sticky Password

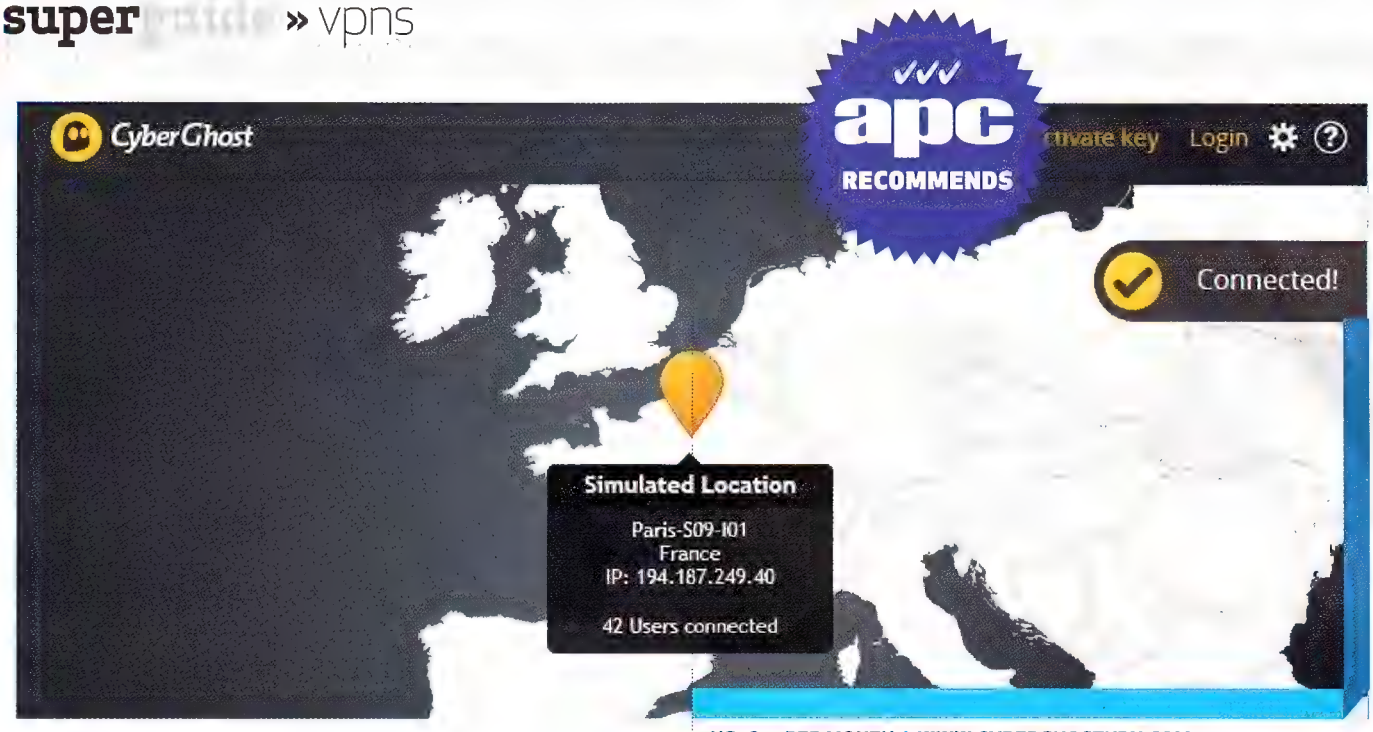
Just another stick-y in the mud.

Most password managers attempt to guilt-trip you into getting their service by flagging scary information about data leaks. Not Sticky though – this password manager just flaunts the fact that it contributes to a foundation that saves manatees. This service can be configured to have online cloud syncing and has its own email authentication system. Though most browser add-ons worked fine, we weren't able to get the Internet Explorer add-on to work on Windows 8.1. However, with no import options, password generator, widgets or browser extensions, the free version is frankly a bit frustrating – so unless you're prepared to buy it without actually having a real trial, Sticky isn't worth the effort. The US $20 per annum sub fee is reasonable, but you can't have more than one account login for any one site or easily replace a password that exists. Despite some of the 'excellent' ratings it gets, Sticky Password isn't overly impressive.

Verdict

A decent application, but with better options out there it's hard to stick with it.

★★★½☆



US$6-11 PER MONTH | WWW.CYBERGHOSTVPN.COM

Protect your privacy with a VPN

Now that the surveillance state is on its way, it may be time to take your online privacy into your own hands. Ashton Mills investigates.

With the advent of mandatory metadata retention laws going into effect in October, George Orwell must be turning in his grave. However, while it's disappointing that our politicians don't actually work for us any more (be sure to kick both major parties to the kerb at the next election) in the mean time you can help protect your privacy – at least as far as internet usage goes – by using a VPN.

Once the domain of educational and business networks, VPNs are increasingly being used to protect people's privacy and in some cases lives in those countries even more draconian than ours. The concept is simple: tunnel to an existing remote network, and route all traffic through it. Along with encryption, it becomes very hard to track your browsing, email and messaging without access to the remote servers.

There are a few features you should look for: whether the service logs activity, though ultimately you have to take their word for it; whether there are Australian servers, so you can use the internet with minimal performance loss; and if it passes the DNS leak test (www.dnsleaktest.com), which is another way you can be tracked by seeing which sites you 'look up' on the internet.

And while you can game over a VPN, you probably don't want to for latency-sensitive games as there will always be an overhead. Note also that many VPN services limit or restrict file-sharing (and those that don't may log data), usually to cover their own legal commitments.

There are many services available, so here's our snapshot of some of the more familiar and less well known products and how they fare.

Cyberghost VPN

Slick interface, good list of features and claims no logging.

CyberGhost VPN touts over 500 servers across 30 countries including Australia to serve your VPN needs. It also boasts a simplistic interface with a big 'power on' button to automatically connect to the CyberGhost VPN network.

By default there are a few tweakable options, including 'anti-fingerprinting' to set a browser's language to the server's origin, and editing the browser OS and version string. You can also try and prevent website tracking and whether these features should be enabled with HTTPS traffic as well.

Beyond this all data is encrypted with 256-bit AES and there are no bandwidth limits, even with the free version.

There are three plans on offer – Free, Premium and Premium Plus. The free plan is free indefinitely, but you have to wait in a queue to join free servers, as well as the number of servers you can access. The speed is also reduced compared to the standard Premium plan, which is limited to one device. The Premium Plus plan extends this to five simultaneous devices.

Device support covers all the bases with clients for Windows, MacOS X, iOS, and Android. Linux is supported through Linux's own OpenVPN toolset. While the native CyberGhost clients use OpenVPN the service also supports IPSec, L2TP and PPTP are also supported.

Finally CyberGhost passed the DNS leak test by utilising its own DNS servers, and the service claims that no logs are stored.

Verdict

Lots of servers and so easy to use your grandma could use it

★★★★½

US$7-10 PER MONTH | WWW.GOLDENFROG.COM/VYPRVPN

VyperVPN

Advanced features for VPN aficionados paired with a clean interface.

VyperVPN's interface is clean and simple, with a large bandwidth graph and the essential settings of remote IP, time connected, and protocol displayed.

As with most of the other VPN products we look at here, VyperVPN uses OpenVPN with 256-bit AES encryption as the protocol, however in the options you can also choose IPSEC, PP2P, and Vyper's own Chameleon protocol which is based off OpenVPN but hides the fact the traffic is VPN traffic. Vyper states this is useful in countries like China where use of VPNs for circumvention may be prevented.

Vyper has its own DNS servers, and passed the DNS leak test, as well as some other welcome security features including stopping all internet traffic when VyperVPN is disconnected, automatically reconnecting on disconnect, and for advanced users the ability to tailor OpenVPN parameters.

As far as plans go there's a free service that has a limit of 500MB bandwidth and 2 simultaneous connections, but otherwise is unrestricted, with the standard fully-featured VyperVPN Pro plan providing unlimited data for US$99.96 annually.

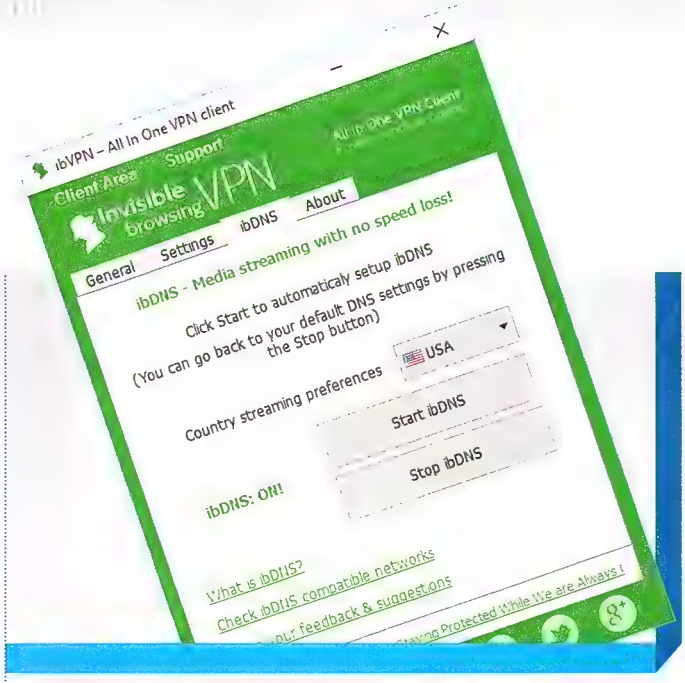
Platform support covers Windows, Mac OS X, iOS, Android, versions even for your router and your TV. VyperVPN also claims no logging of its VPN service or its DNS servers. Servers are available in Australia, too.

Using your account to log in allows you to manage your service as well as add other Vyper services which include Dump Truck online storage and Cypher encrypted messaging.

Verdict

Pricey, but feature rich and ticks all the boxes.

★★★★☆



$US3-5 PER MONTH | WWW.IBVPN.COM

ibVPN

Not as slick as the others but one of the cheaper services

ibVPN's interface isn't a slick as some of the others we cover here, but it has all the essential features. This includes being able to select a preferred server, the protocol (which includes OpenVPN, L2TP, PPTP and SSTP), and toggling Auto Reconnect and Kill Switch options (which automatically closes select applications if the VPN link is lost).

By default ibVPN doesn't enable its ibDNS service, you have to manually start it, and it passes the leak test. It can also be used independently, and can be purchased as a separate product as a means to bypass geoblocking (for e.g., streaming media from BBC UK or US Netflix from Australia).

In terms of plans there's a free trial that lasts six hours, but is otherwise unrestricted, along with two ibVPN plans capping at the Ultimate VPN price of $US58.08 for a year. Another plan provides just the ipDNS service for streaming, while a fourth plan curiously is designed for torrent users. While the terms of use prohibit use of the VPN network for illegal torrenting, it does state the torrent servers are limited to Luxembourg, Sweden, Netherlands, Canada, Russia and Hong Kong. Curiously out of jurisdiction of litigation-heavy USA.

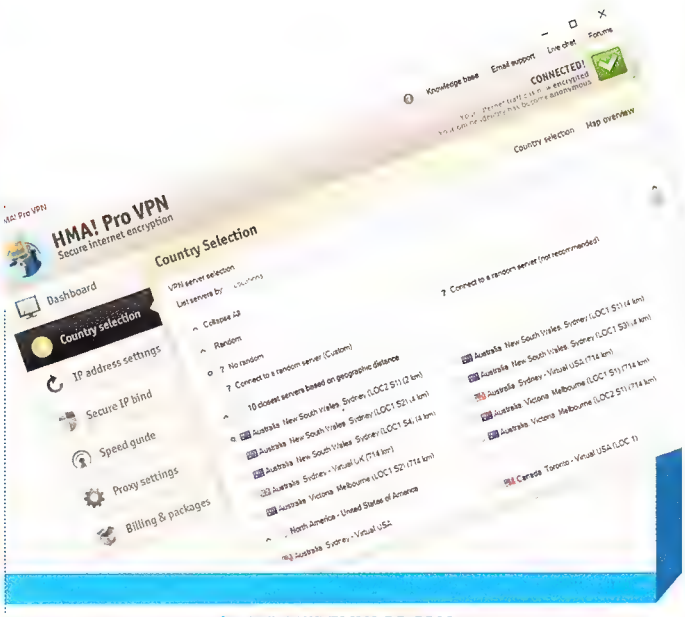
ibVPN claims 94 servers across 39 countries, including servers in Australia, and while it states it doesn't log internet usage it does plainly say that connection and bandwidth data is kept for seven days. Clients are available for Windows, Mac OS X, iOS, Android, Linux and some routers (including DD-WRT based routers).

Verdict

Not as many servers to choose from, but it's also less expensive.

★★★☆☆

$US4-7 PER MONTH | WWW.TUNNELBEAR.COM



US$6-11 PER MONTH | WWW.HIDEMYASS.COM

TunnelBear

Who knew you could making using a VPN cool?

Easily the coolest VPN client we've seen, making use of a grizzly bear meme to keep it light and friendly. Any tool that features lasers coming out of bear eyes destroying trackers during setup gets a thumbs up in our book.

The interface is as simple as it gets – choose a country, and turn it on. Optional settings allow you to enable 'Maul Trackers' mode, a 'Vigilant' mode that ensures all network activity is stopped in the event a connection is lost and restarted (eg if you're using an unreliable Wi-Fi connection), and a TCP override mode which forces TCP in place of UDP in case ISPs throttle UDP traffic.

You can also define inclusion or exclusion lists of websites that should or should not use the VPN if you dig into Tunnelbear's 'Intellibear' mode (for example, adding your bank's website to the exclusion).

Plans are divided into 'Little' bear, a free 500MB per month plan; Giant bear for $US7 a month and supports up to five devices; and Grizzly Bear, which is exactly the same plan but billed year to save money, coming in at US$50 a year.

Tunnelbear claims no logs are kept, OpenVPN is used for the protocol, and all data is encrypted with 256-bit AES. On the surface Tunnelbear fails the DNS leak test, which while not utilising your ISP's DNS servers, instead uses Google DNS servers (which are going to be logged). However TunnelBear's FAQ explains that DNS requests are sent via TunnelBear, and so will appear to come from TunnelBear's servers.

Clients are available for Windows, Mac OS X, iOS and Android as well as Chrome.

Verdict

Despite the basic interface, Tunnelbear is versatile and effective.

Hide My Ass!

One of the more popular VPNs with a wide range of servers.

The inventively titled Hidemyass! VPN boasts an impressive 890 servers in 190 countries for US$80 a year for a 12-month subscription.

The client certainly isn't as flash as something like VyperVPN or Tunnelbear, and despite the range of options in the left menu and digging deeper into the settings, doesn't offer much more than a tunnelling VPN service. The main options you can toggle are randomly changing IP address on a schedule, and binding particular applications to your VPN IP so they only operate when the VPN is active. A connection log is also visible, though this isn't particularly handy for most people, and the ability to choose between OpenVPN and PPTP protocols. Beyond this the most useful feature is the Speed Guide that shows the servers closest to you.

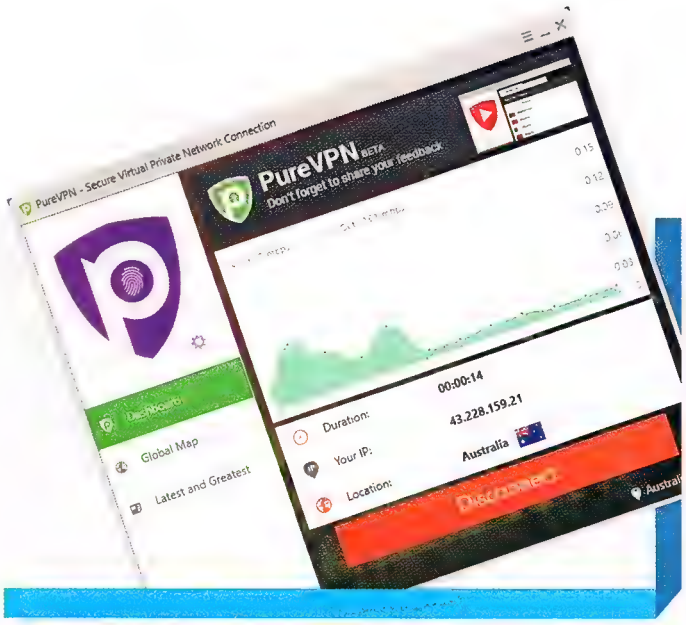
Hidemyass! doesn't have its own DNS servers and it failed the DNS leak test, with some requests being diverted to OpenDNS and others to our ISP's DNS servers, meaning websites we visit will be logged according to the ISP's policies.

Clients are available for Windows, Mac OS X, iOS, and Android. Connection with Linux can be managed through Linux's OpenVPN tools.

Hidemyass! offers a number of other services, including anonymous email, a web proxy and business VPN. It's one of the more expensive of the VPNs we looked at here, with its biggest advantage being the scope of servers available, and which include a number in Australia.

Verdict

Another one for more advanced users, and a little on the expensive side.



US$4-10 PER MONTH | WWW.PUREVPN.COM

PureVPN

Pre-defined 'modes' try to make VPN easier for the masses.

When first running the PureVPN client it prompts whether you want to use the service for streaming, privacy, or file sharing among other options and pre-configures the client accordingly (for example, not all servers support file sharing, so you won't connect to these). Apart from this the interface is clean and simple, with a bandwidth graph showing usage. Servers can be selected from a drop down and, when selecting a country, will try for the fastest server.

Options are few but include auto-reconnect on connection loss, a kill switch to disable all internet activity if the connection is lost, the option to change protocol (and which includes L2TP, SSTP, PPTP and IKEv), and the ability to use weaker encryption or disable it entirely for faster performance.

PureVPN failed the DNS leak test even when choosing 'Switch to Secure DNS' under the Advanced options, and which requires running PureVPN with Administrator privileges.

Though the price seems good some of the extra services, such as NAT firewall or Smart DNS for streaming media, are sometimes offered by other VPNs free. The 12-month plan comes to US$50 and the service claims 500+ servers in 141 countries including Australia.

Clients are available for Windows, Mac OS X, iOS, Android as well as compatibility with a range of routers. It also claims no logging of any sort.

Verdict

Simple interface, essential features and cheap if paid annually.

★★★☆☆

US$7 A MONTH | WWW.PRIVATEINTERNETACCESS.COM

Private Internet Access

No frills VPN with a huge number of servers.

Private Internet Access sports by far the most basic interface, providing an application to configure the core settings and no extra frills like a bandwidth monitor (not that you need this). Instead, right-clicking on the program in the notification area allows you to connect to servers around the world, and you're done.

Settings include enabling DNS leak protection (using its own DNS servers, and it passed the DNS leak test), IPv6 leak protection, a VPN kill switch to stop network activity on a disconnect and port forwarding – useful if doing file sharing. Beyond this you can set the encryption level for data, authentication, and the handshake, in order to set your preference of security vs speed, and then that's about it as far as settings go.

Private Internet Access claims a whopping 2,897 servers spread across 20 countries, and includes servers in Australia in Sydney and Melbourne. It also claims a no logging policy, and features an 'NSA Re-education' page on the site that outlines the risk to information as seen by PIA.

Protocols support cover OpenVPN, PPTP, and L2TP and there are clients are available for Windows, Mac OS X, iOS and Android, and Ubuntu Linux along with instructions for configuring it for some routers.

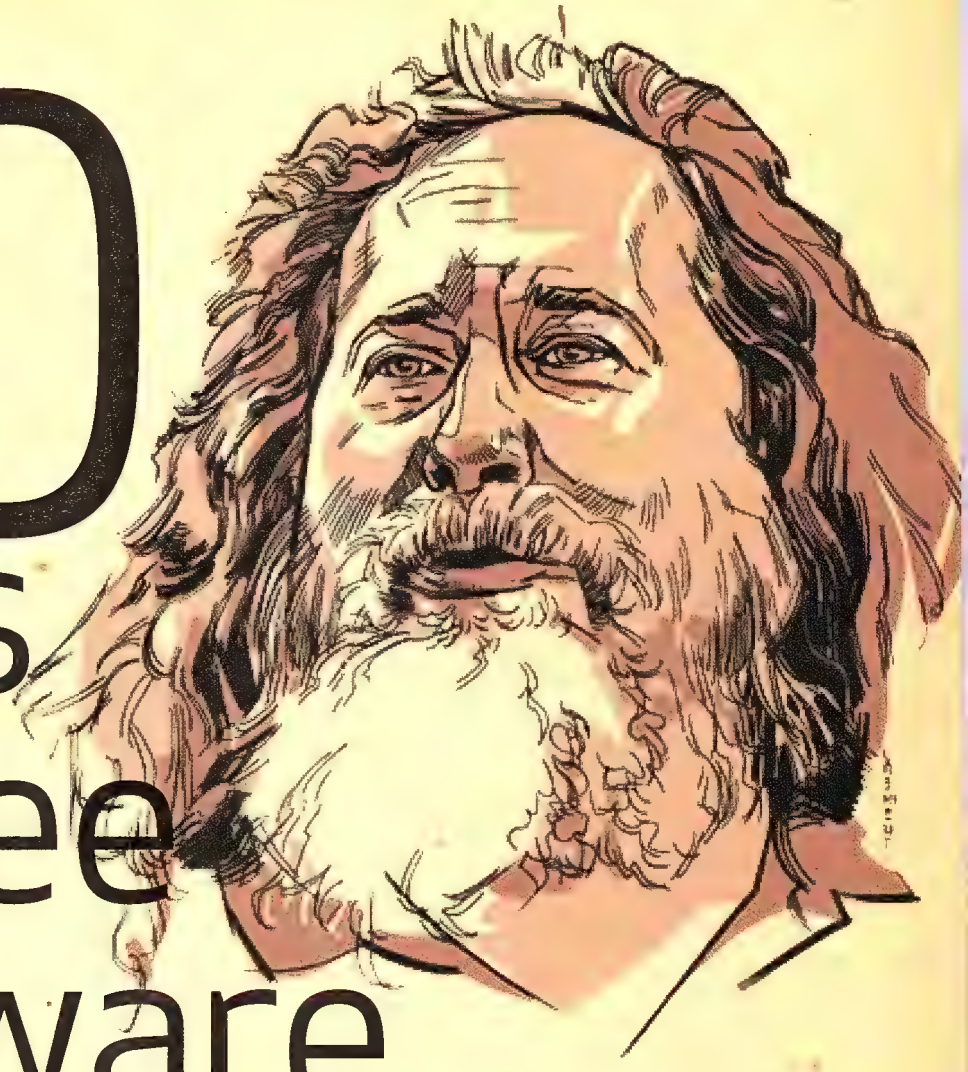
Plans start at US$7 a month, or US$40 if paid 12-months in advance, for up to five simultaneous devices making it one of the cheaper products we looked at here.

Verdict

Basic interface but cheap while providing a good selection of regions.

★★★★½

30 years of free software



Jonni Bidwell delves into the origins of free software and reminds us that much of our software freedom is due to the efforts of a single, hairy hacker.

Freely licensed open source software (FLOSS) is largely running the internet, as well as some *APC* writers' home machines (and maybe even some of their brains too). Free software was relatively common throughout the '60s and early '70s too: programmers (rarer and even hairier than today's species) typically worked on leased mainframes that came with source code provided (although IBM eventually put the kybosh to this practice). Academicians co-opted one another's code in the name of not re-inventing the wheel, and likely never gave credence to the idea of privatising or monetising their programs.

Bill Gates' 1976 Open Letter to Hobbyists, (**http://go2.pt/jAGeja**) besides making people feel bad for pirating BASIC, engendered the idea that all software should be paid for, and its source code kept from prying eyes. The burgeoning microcomputer industry shared Gates' sentiment and proprietary software quickly became the norm. Meanwhile communications giant AT&T, who had hitherto provided the Unix OS to governments and universities for free, were forced by deregulation proceedings to commercialise it.

"Academicians co-opted one another's code in the name of not re-inventing the wheel."

Richard Stallman claims that his musings on software freedom began at the AI LAB at MIT. For years hackers there had fought with a rogue Xerox printer that had a propensity for paper jams. Having access to the Unix printer driver source enabled them to get the printer to email everyone in the print queue whenever it had jammed, so that whoever was closest could fix it. This printer was later replaced, but soon, like its predecessor, it became prone to malfunctions. Unfortunately no driver source was bundled with this device, and Stallman's attempts to ascertain a copy of it were met with a blank refusal. This stood firmly against the co-operative hacker culture he held sacrosanct and one score and twelve years ago he was spurred into action.

The GNU Manifesto aimed to paint a different future for software

Stallman announced the GNU (GNU's Not Unix) Project in September 1983. The ambitious goal was, through a mass-collaboration effort, to produce an operating system called GNU, that was entirely free. Stallman's definition introduced four basic freedoms (which are laid out in the 1985 GNU Manifesto – **http://bit.ly/GNUManifesto** and below) of which all users ought to be entitled.

There is potential for linguistic ambiguity between cost-free ('gratis') and free ('libre') here. First, note that the freedoms depicted (see bottom of page) make no mention of any monetary conditions. None of these freedoms place any restrictions on selling the software, so it's perfectly reasonable for free software to have a price tag. Conversely, a software program made available at no cost can quite easily fail to provide the above definition of freedom: e.g. freeware titles that don't include source code or open source code that runs on a machine which checks for and refuses to run modified versions of that code. Certainly having the source available is a precondition to Freedoms 1 and 3, but if the creator then prohibits modifications or (more likely) allows modified versions to be redistributed as part or whole of a proprietary program, then they fall foul of the freedom police. Such behaviour violates the copyleft principle since the derivative product will be released under different conditions to the original software.

The term 'open source' was inaugurated with the formation of the Open Source Initiative (OSI) in 1998, partly as a means of disambiguation, but partly to distance the OSI from the Free Software movement. The prevailing feeling amongst the OSI was that the maverick image associated with the Free Software camp would deter businesses from adopting or contributing to open source software. The original OSI definition for Open Source was based around the Debian Free Software Guidelines (DFSG) and as such contains provisions other than availability of source code.

In fact, at face value, the OSI and Free Software movement definitions have much in common, but they originated from very different philosophies. The latter is couched in much more pragmatic language than the perceived anarchistic tones of the former. The OSI wanted businesses to be more amenable to strategies like that of Netscape, who published the code for its Communicator suite in 1998.

The four paths to open-source freedom

FREEDOM 0 ::
Freedom to run the program as you wish, for any purpose.

FREEDOM 1 ::
Freedom to study how the program works, and modify it to suit your purposes.

FREEDOM 2 ::
Freedom to redistribute copies of the program.

FREEDOM 3 ::
Freedom to publish your own modified versions.

Stallman's alter ego, St. IGNUcius may be a bit of light-hearted fun, but the goals of the Free Software movement are not

Genesis of the GNU Project

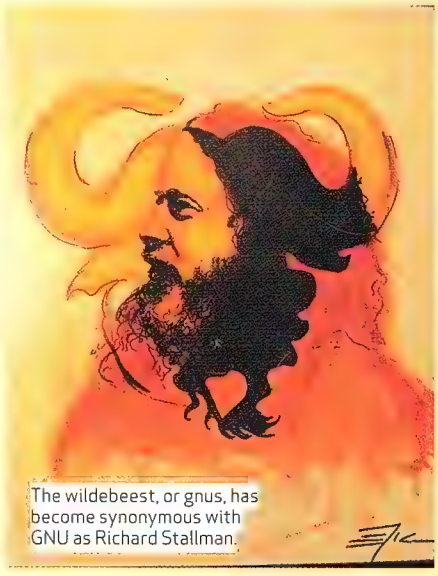
Stallman began work on one of the key components of GNU, a version of the Emacs text editor, in 1984. Other tools followed swiftly after: the GNU compiler collection (GCC) and GNU debugger (GDB), as well as rewrites of the myriad Unix command-line tools (ls and friends) nowadays taken for granted by Linux users. Concerned that his employer may try and claim copyright of GNU assets, Stallman resigned his post at the AI Lab. MIT apparently took no offence at this and continued to allow him access to their computing facilities.

The GNU OS, Stallman decided, would have to be compatible with Unix. This meant that GNU would automatically inherit Unix's portability and that some free Unix software (such as the TeX typesetting system, and later the X Windows System) could easily be incorporated into GNU. It also meant that once the project had grown to involve developers in multiple locations, they didn't need to be so much concerned about compatibility: if their contribution was compatible with Unix, then it would be compatible with GNU OS.

"The GNU GPL has proven to be much more than an idealistic screed."

Through the GNU project, Stallman hoped to effect a social movement through technical means. But this radical departure would have to take place in such a way as to respect existing copyright law, which was (and still is) framed around protection and limitation rather than the liberation and promiscuity trumpeted by the GNU camp. The document which permitted this change would eventually come to be known as the GNU General Public License (GPL), but in its infancy it was just the Emacs General Public License. The critical hit in this document was the stipulation that while modifications and derivative works were permitted, those modifications would have to be released under the same Emacs licence. Proprietary offshoots were absolutely verboten. The arrangement became known as 'copyleft' – which used traditional copyright law to serve something like the inverse of its intended purpose, and grant users permission to copy, modify and distribute software but denying them the right to add any restrictions.

Stallman formed the Free Software Foundation (FSF) as a non-profit organisation in 1985 to support the GNU movement. In the early days, the FSF generated revenue through the sale of the hefty manuals that explained how Emacs worked, as well as, perhaps counter-intuitively, copies of the software itself. And here we run into the oft' quoted epithet 'free as in speech as opposed to free as in beer'. There is absolutely nothing in the GPL that prevents anyone from selling GPL-licensed software. Just as well really because that's exactly what the FSF was doing. In a pre-web era this made a modicum of sense – most people couldn't just jump on the ARPAnet and FTP to the AI lab. Other channels also sold GNU software, in many cases undercutting the FSF (and this was perfectly legal too), but the FSF found that people were willing to contribute to them simply because customers appreciated the work that they were doing. First, the FSF sold software on tapes, then disks and finally CDs. This distribution service provided most of the FSF's funds over the first decade. Today they remain the principle organisational sponsor of GNU, but are largely funded through donations and memberships, the FSF also has some merchandise for sale (**shop.fsf.org**) including the Emacs manual, which is now in its 17th edition and running to 651 pages. You can also download it for free at the same site.



The wildebeest, or gnus, has become synonymous with GNU as Richard Stallman.

The quest to finish GNU is technically still ongoing, and some readers will be aware that development of The Hurd (GNU's kernel) did not proceed at the same pace as the userspace. Then in 1991 a certain Finn popped up on Usenet inviting everyone to try his own Linux OS. Unlike GNU, Linus Torvalds' Linux had a complete and working kernel (though only for 386 machines) and the GNU tools were naturally ported to it. Linux 0.12 was released under the GPL and the GNU/Linux combination constituted the world's first libre operating system.

The GPL has proven to be much more than an idealistic screed. Harald Welte, principal developer of the iptables kernel subsystem, created the **gpl-violations.org** website (Note: which is no longer active) in 2004 to assist copyright holders in action against GPL infringements. Welte's efforts resulted in a number of court victories, showing that the GPL does indeed have teeth. Today legal representation for FLOSS developers is provided pro bono by the Software Freedom Law Center (**www.softwarefreedom.org**) and the Software Freedom Conservancy (**sfconservancy.org**) provide support to affiliated developers. Most recently the SFC have been supporting Christopher Hellwig's GPL-compliance suit against VMware.

Stallman on...

RMS is known for his uncompromising stance on matters of freedom and copyright. Sometimes these run counter to popular interpretation, but if you care about freedom, it's worth familiarising yourself with the philosophy of the bearded renegade. You'll find a number of his essays at **https://gnu.org** and on his own website **https://stallman.org**.

Free software:

"When we speak of free software, we are referring to freedom, not price."

Free vs open source:

" The two terms describe almost the same category of software, but they stand for views based on fundamentally different values. Open source is a development methodology; free software is a social movement ... We in the free software movement don't think of the open source camp as an enemy — the enemy is proprietary (non-free) software. But we want people to know we stand for freedom, so we do not accept being mislabelled as open source supporters."

Stallman's law:

"...in an epoch when governments work for the mega-corporations instead of reporting to their citizens, every technological change can be taken advantage of to reduce our freedom. Because reducing our freedom is what these governments want to do."

Software piracy ::

"...The example of the struggling artist is a ridiculous example because the existing system does very little for struggling artists. It's lousy. And if we just legalise sharing it won't make any difference to [them]. It might even help them."

Linux:

"Many users do not understand the difference between the kernel, which is Linux, and the whole system, which they also call 'Linux' ... Programmers generally know that Linux is a kernel. But since they have generally heard the whole system called 'Linux' as well, they often envisage a history that would justify naming the whole system after the kernel. For example, many believe that once Linus Torvalds finished writing Linux, the kernel, its users looked around for other free software to go with it, and found that (for no particular reason) most everything necessary to make a Unix-like system was already available... What they found was no accident — it was the not-quite-complete GNU system."

Patent law vs copyright law:

"These laws originated separately, evolved differently, cover different activities, have different rules, and raise different public policy issues. Copyright law was designed to promote authorship and art, and covers the details of a work of authorship or art. Patent law was intended to encourage publication of ideas, at the price of finite monopolies over these ideas – a price that may be worth paying in some fields and not in others. Trademark law was ... simply to enable buyers to know what they are buying."

DRM:

"The motive for DRM ... is to increase profits for those who impose them, but their profit is a side issue when millions of people's freedom is at stake; desire for profit, though not wrong in itself, cannot justify denying the public control over its technology. Defending freedom means thwarting DRM."

Text editors:

"It's true that vi is the editor of the beast, but using a free version of vi is not a sin, it's a penance." ■

how to...

» QUICK TIPS

Experts solve your computing problems

APC and its readers can be one giant helpdesk. If you have a technical problem, chances are one of us can solve it.

RASPBERRY PI

CROCODILE TEARS

I've just started experimenting with the Raspberry Pi. I'm comfortable with the programming side, but the electronics aspect is all new to me. I'm not sure how much I need to worry about static electricity. If I want to test a part like an LED, is it OK to just wind the wire around the output pins on the Pi, or do I need to a set of crocodile clips?
Mark Crewkerne

Provided you're careful not to short out any of the adjacent pins, wrapping wire around a pin, or just holding the legs of the LED directly to the Raspberry Pi pins won't damage anything. Static can be a problem in a carpeted room, unless you're wearing an earthed wrist strap. But sat at the kitchen table you'll be completely fine.

But wrapping wire around pins is a bad idea for a completely different reason. It's a really unreliable way to make a connection. As soon as your circuit gets more complicated than battery > resistor > LED > pin, you'll spend all your time wiggling joints to make sure they really are connected. If you are used to the deterministic nature of programming bugs, this sort of intermittent error will drive you potty. Get a breadboard and some jumper leads from an electronics shop and use mini crocodile clip test leads to connect from your breadboard to the Pi. You can get cheap sets of 10 for under $10, so it's hardly much of an investment.
Luis Villazon

HARDWARE

A VAIN HOPE

My laptop (an HP Pavillion) recently refused to boot. I tried the Windows Startup Repair and when that didn't work I also tried System Restore. That didn't work either.

I've taken the drive out and put it in a USB drive caddy to run some diagnostics from my desktop PC. This gives me a clean bill of health except for one error: 'Raw Read Error Rate: Threshold value 51, Current value 1, Worst value 1.' I've done some reading up and this seems to come from the SMART monitoring software.

Is there some way I can reset this error count or increase the threshold to get the drive working again? I can put up with one or two read errors if it means I get the rest of my data back.
JP

That's unlikely to fix the issue unfortunately. Imagine there's a fireman hosing down the embers of your recently ablaze house. Asking him if he can take the battery out of your smoke alarm isn't really tackling the heart of the problem.

"Imagine a fireman hosing down the embers of your recently ablaze house. Asking him to take the battery out of your smoke alarm isn't tackling the problem."

A set of mini crocodile clips is essential when you're playing around with Pi hardware hacking.

SMART stands for Self-Monitoring, Analysis and Reporting Technology. It doesn't disable your hard disk, it just tries to tell you what's wrong with it before it fails altogether. And in your case it hasn't even managed to do that, because your disk has already failed. That read error is well below the warning threshold, which means that something else broke – and broke so quickly that SMART unfortunately didn't have time to warn you about it.

SMART can warn you about failing hard drives... if you're lucky.

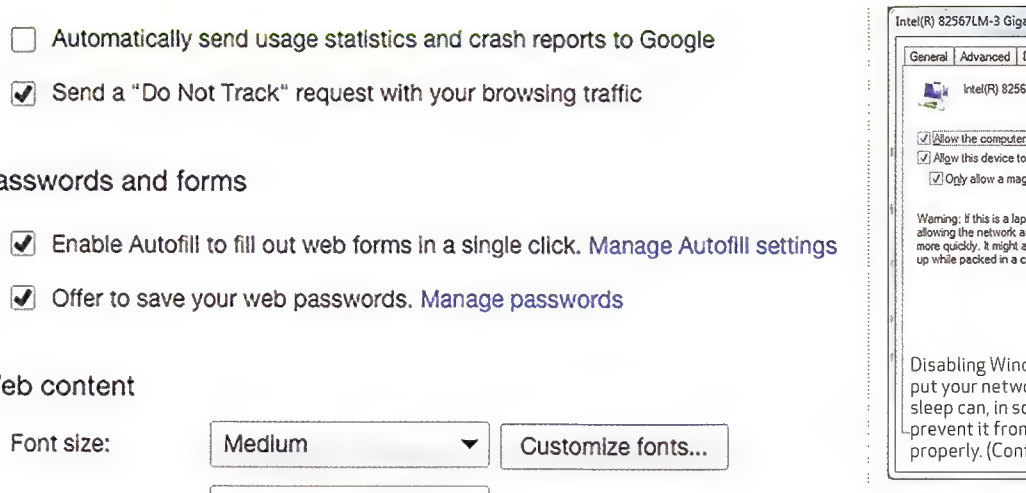
SMART may well be clever, but I've never known anyone who has had their data saved by it. Most people either aren't warned in time, or ignore the warning when it comes. And the few that are cautious enough to listen already make regular backups, and so don't need it.
Luis Villazon

INTERNET

AUTOFILL ANARCHY

I'm a big fan of Google Chrome and greatly prefer it to all the other browsers but there is one thing that is driving me mad: where is 'autofill' data, such as addresses and credit card numbers stored? I've downloaded DB browser for SQLite and gone through all the likely-looking files in /Appdata/Local/Google/Chrome/User Data/Default but so far I've come up empty! Is this data actually stored in the cloud?
Jonathan Btembi

I think the folder you mention has been used in the past for Chrome autofill data, but there's no requirement for Google to preserve backwards compatibility in this regard. Certainly there doesn't seem to be anything there on my installation now. Google could easily have moved this into the cloud, and it would probably be safer if it did. But anyway, there's no reason to manually open each database file, because Chrome handily has a user


Automatically send usage statistics and crash reports to Google
Send a "Do Not Track" request with your browsing traffic
Passwords and forms
Enable Autofill to fill out web forms in a single click. Manage Autofill settings
Offer to save your web passwords. Manage passwords
Web content
Font size:
Medium
Customize fonts...
Page zoom:
100%
Pressing Tab on a webpage highlights links, as well as form fields
Network
Your network proxy settings are being managed by an extension.

If you need to change Chrome autofill entries, you can do so from within Chrome's own Settings menu.

interface option that does exactly this. Open Settings, scroll to the bottom and click 'Show advanced settings...' Under 'Passwords and forms' you can click 'Manage Autofill settings' or 'Manage passwords'.
Luis Villazon

WINDOWS
GROGGY ON RISING

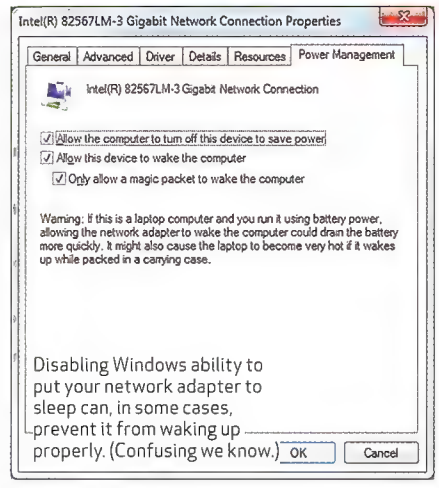
I have a Windows 7 laptop that normally goes into standby after half an hour. Whenever I wake it up, whether it's after several hours or straight away, it's lost the Wi-Fi connection. I have to right-click the Wi-Fi icon and reconnect manually — if I leave it alone it will never reconnect by itself. This is extremely annoying. I can obviously disable standby mode ltogether, but it kills my battery. I've been through all the power management settings and made sure they're all on 'Maximum Performance', but this has made no difference at all.
Jean Gearies

Clicking one extra icon every 30 minutes, at most, logically ought to be something we could laugh off – it's roughly the same amount of energy as you will expend today digging interesting crusty bits out of your ear, or opening the microwave door a second early, so you don't have to listen to all the beeps. But what is so maddening is not the effort involved, it's the pointlessness of it. This seems like such a simple problem to solve. The PC knows which network you normally connect to; why doesn't it just reconnect automatically without being asked?

Well, if you think that's infuriating, take a deep breath. This fault is actually a bug in many Intel Wi-Fi drivers, and it's caused precisely by the efforts you've been taking to prevent it happening. By clearing the checkbox in Device Manager that says 'Allow the computer to turn off the device to save power' for your Wi-Fi adaptor, you've been stopping the driver from spotting that the power was cut anyway when the whole laptop went into standby mode, so it doesn't restore your connection when the power comes back on. So if you tell it not to turn off, it does. If you do let it turn off, however, it will silently reconnect fast enough that it feels as if it actually stays on all the time!
Luis Villazon

HARDWARE
TIME TO UPGRADE?

I'm wondering how much longer my systems will hold up against all of the new games/software out there. Back in 2011 and 2012, I built two desktop PCs. Both are running on LGA 1155 interfaces. They're almost identical except for their CPUs. One has an Intel Core i7-2600K (Sandy Bridge) quad-core processor, while the other has a Core i7-3770K (Ivy Bridge). Each machine has 32GB of DDR3-1600, Mushkin 240GB SSDs, and a Gigabyte GV-N970G1 GAMING-4GD GeForce GTX 970. How much longer will these systems be able to run today's games at max settings? We're currently playing MechWarrior Online and Elder Scrolls Online. With all of the CPU power available now, would it be best to upgrade soon, or do I still have a few years of great gaming in store?
Robert Klaas


Intel(R) 82567LM-3 Gigabit Network Connection Properties
General
Advanced
Driver
Details
Resources
Power Management
Intel(R) 82567LM-3 Gigabit Network Connection
Allow the computer to turn off this device to save power
Allow this device to wake the computer
Only allow a magic packet to wake the computer
Warning: If this is a laptop computer and you run it using battery power, allowing the network adapter to wake the computer could drain the battery more quickly. It might also cause the laptop to become very hot if it wakes up while packed in a carrying case.
Disabling Windows ability to put your network adapter to sleep can, in some cases, prevent it from waking up properly. (Confusing we know.)
OK
Cancel

You're being modest there, Robert. Those were the fastest CPUs available when the Sandy Bridge and Ivy Bridge architectures launched. And if we're being honest, Intel didn't improve host processing performance much from one generation to the next (that includes its Haswell and Broadwell efforts, by the way).

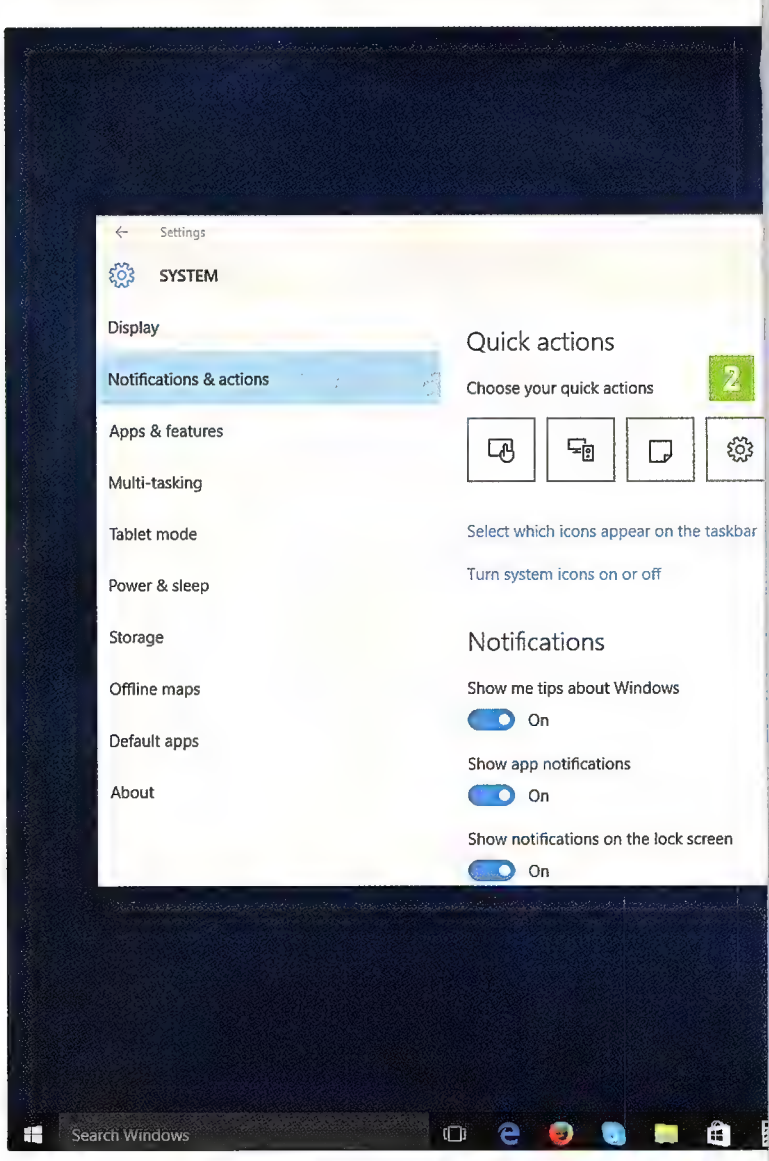
On top of that, you're rocking tons of memory, speedy SSDs, and some of the fastest single-GPU graphics cards available. It helps that the games you're into aren't resource hogs. We're missing a bit of information, though. What resolution do you game at? Do you have an urge to see what 4K is all about? Do your motherboards support two-way SLI, at least?

More than likely, those two machines will serve you well for another couple of years. If you start noticing slow-downs at maxed-out settings, suspect your graphics cards first. Fortunately, adding another GTX 970 is a lot cheaper than starting from scratch.
APC team

Even an older Ivy Bridge (aka third-generation) Core i processor can still handle modern gaming with the right graphics card.

Stay notified in Windows 10

"Windows 10's new Action Centre puts notifications at your fingertips. Nick Peers explains how it works.



One of Windows 10's most radical changes is the way in which it provides notifications. Previously you'd see a little white flag appear in the Taskbar's notification area, with a pop-up balloon on hand to keep you informed. Now notifications are much more visible thanks to the new Action Centre, which appears on the right-hand side of your desktop.

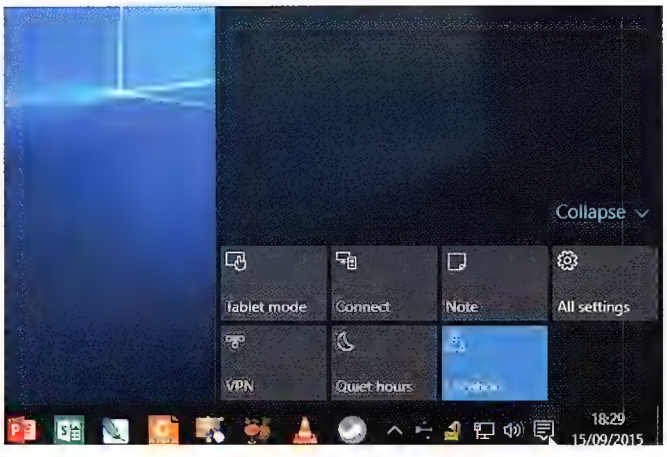
It's now primarily concerned with delivering notifications, both from Windows and supported apps, but it also contains a number of useful shortcuts in the form of action buttons. Up to 13 different buttons are available, but many like Rotation lock, Airplane mode and Bluetooth will only appear on portable devices like laptops or tablets. In this tutorial we'll show you how to navigate the Action Centre, plus customise it to show only those notifications you actually want to receive.

Use and customise Action Centre

USB device not recognised
The last USB device you connected to this computer malfunctioned and Windows does not recognise it.
17:58
15/09/2015

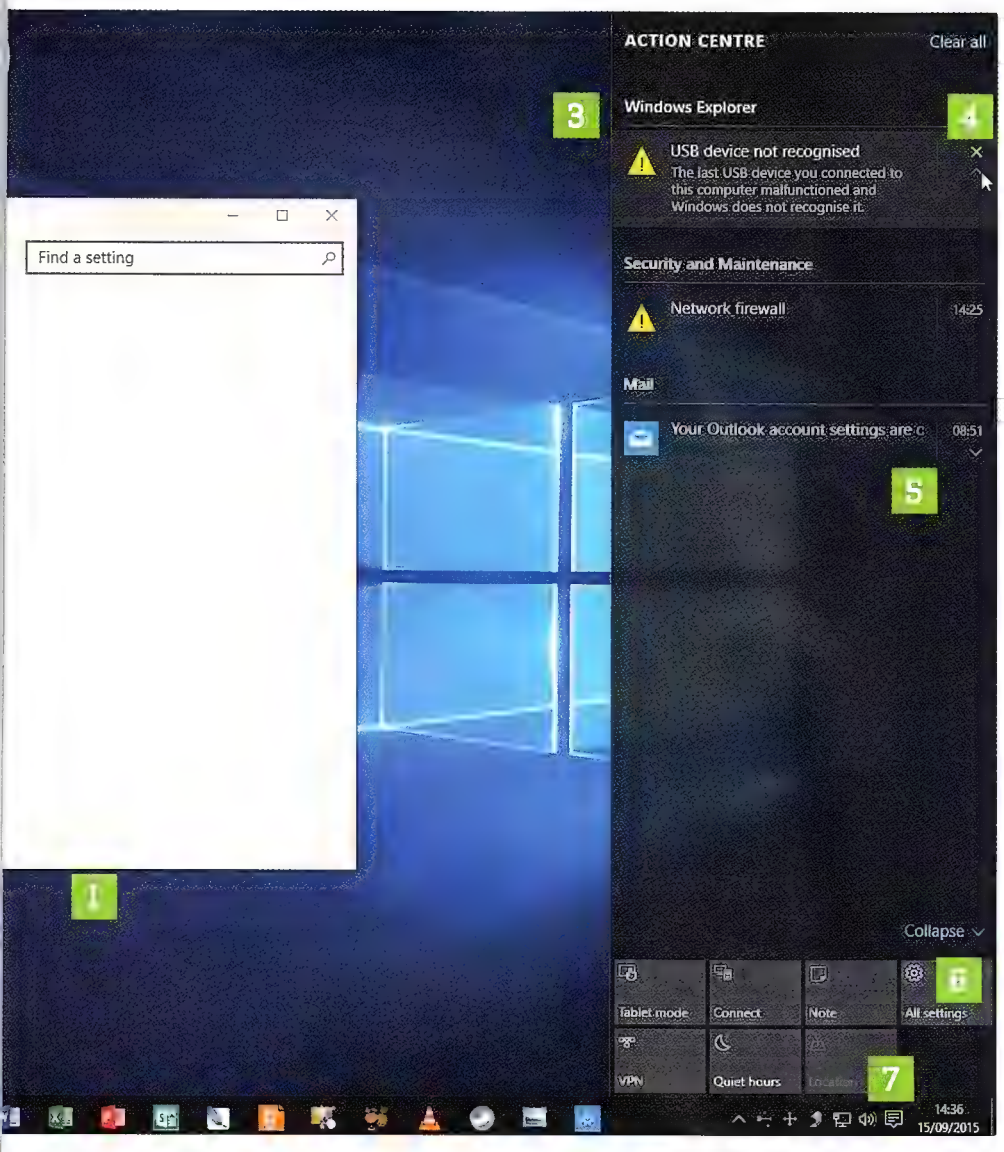
1 NOTIFICATION BANNERS

Individual notifications will — by default — slide out on-screen just above the Taskbar Notification area, accompanied by a sound. If you want to respond to this notification banner, try clicking it — it'll hopefully launch the correct app or system setting for you to take action. After a short pause the notification will disappear, or you can click the close button to dismiss it.



2 OPEN ACTION CENTRE

Look for the Action Centre's icon in the Notification area of the Taskbar — it's the speech bubble icon. Clicking this will slide the Action Centre itself into view, complete with list of recent notifications. Navigating it is relatively straightforward — use the annotated screenshot above to help if necessary. Click anywhere else on-screen to hide it from view again.



1 TWEAK SETTINGS
The Action Centre's settings can be found in the System section under 'Settings'.

2 ACTION BUTTONS
These buttons give you quick access to useful settings, plus allow you to pause notifications and reminders during 'quiet hours'.

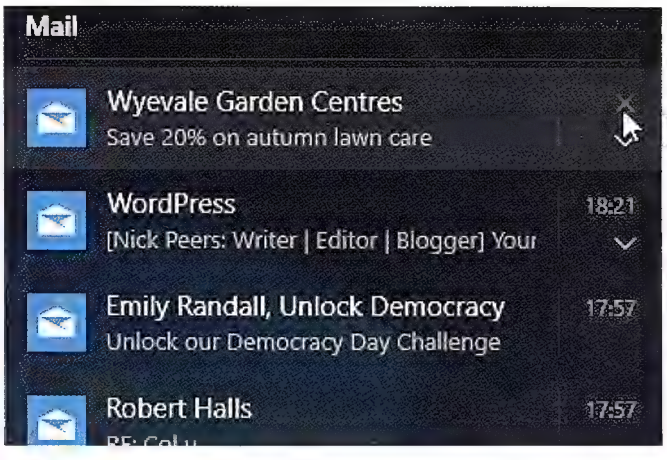
3 NOTIFICATIONS
Notifications are clustered together, grouped by parent app or system setting.

4 TAKE ACTION
Click a notification to interact with it, or click the 'X' button to remove it permanently from the list.

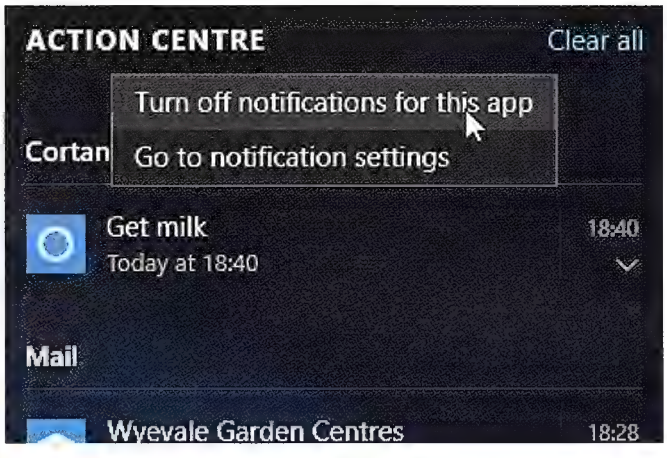
5 VIEW IN FULL
Roll your mouse over a notification and click the down arrow button to show its full contents. Click the up arrow to collapse it again when done.

6 TASKBAR NOTIFICATION AREA
Previously known as the 'system tray', this is the area of the taskbar where icons are displayed by programs and Windows to provide status updates and other useful info.

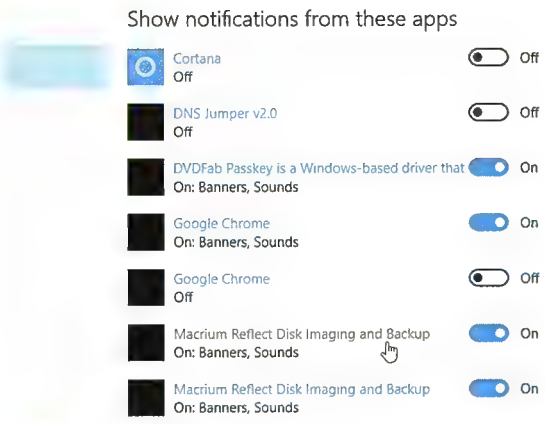
7 ACCESS THE ACTION CENTRE
Just click this button to bring the Action Centre into view, or press Windows-A to show or hide it.



2 REVIEW NOTIFICATIONS
When the Action Centre is open, a summary of each notification — organised by app or type — is displayed in a chronological list, with the most recent notification at the top. Some notifications disappear automatically the next time the Action Centre is closed, while others will stick around. Manage these in the same way you would individual notification banners.

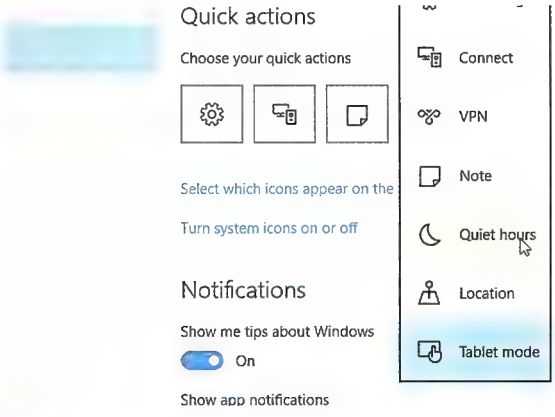


4 MANAGE NOTIFICATIONS
At the present time, few apps use the Action Centre, but as new updates are released it's likely more and more will switch to using this rather than their own notification systems to grab your attention. If you're unhappy receiving notifications from a particular app in this way, simply right-click a notification in the list and choose 'Turn off notifications for this app'.



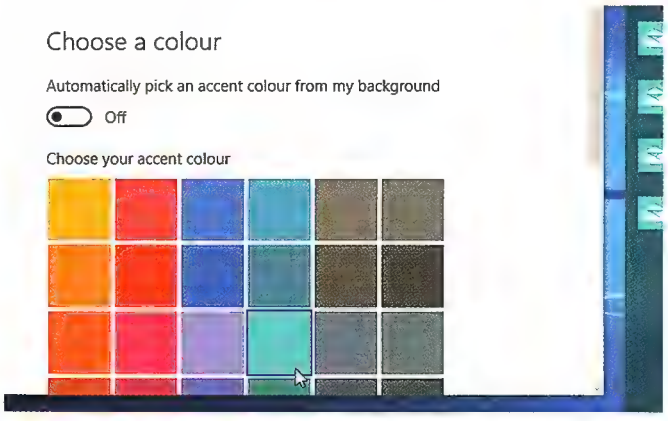
5 CONFIGURE NOTIFICATIONS BY APP

Click 'Start > Settings > System > Notifications & actions'. Scroll down to the 'Show notifications from these apps' section. Use the switch next to each app to enable or disable notifications for that specific app, or click the app name to disable the slide-out banners and notification sounds it makes without switching off notifications altogether.



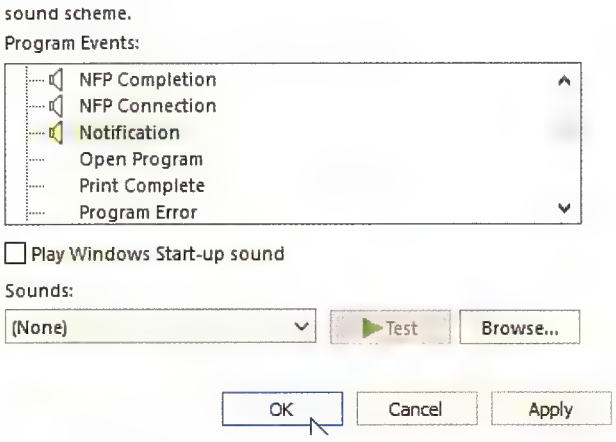
7 ACTION BUTTONS

You'll notice a number of handy shortcut buttons at the bottom of the Action Centre. If they're taking up too much room, click the 'Collapse' button above them to hide all but the top four buttons. You can configure which four buttons are shown via 'Settings > System > Notifications & actions'. Click a button and choose a replacement for it from the drop-down list.



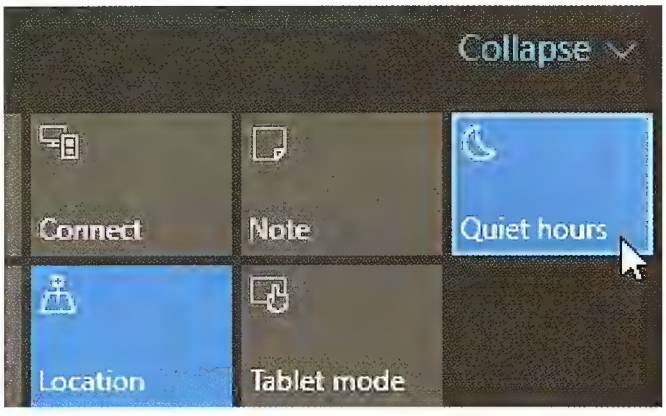
9 CHANGE COLOUR SCHEME

The Action Centre — along with the Start menu and Taskbar — utilise a black colour scheme by default. You can make this match your background: click 'Start > Settings > Personalisation > Colours' and flick the 'Show colour on Start, taskbar and action centre' switch to 'On'. Flick 'Automatically pick an accent colour…' to 'Off' if you'd like to choose your own colour scheme.



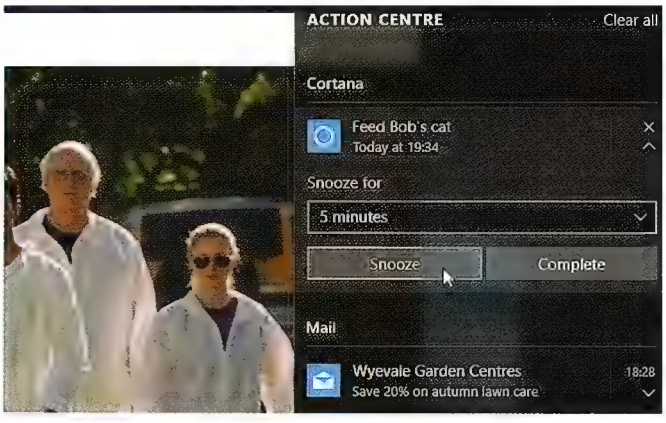
6 CUSTOMISE NOTIFICATION SOUND

If you'd like to change (or disable) the sound made when a notification arrives, type `sound` into the Search box and open Sound Control Panel. Switch to the Sounds tab, scroll down the Program Events window and select Notification. Now click the Sounds dropdown menu and choose a different sound or select (None) to disable it. Click OK to make the change.



8 ENTER A QUIET ZONE

Notifications can be distracting, so it's handy to know you can temporarily disable them completely with a single click: to do so, open the Action Centre and click the 'Quiet Hours' button. When you're ready to switch them back on, click 'Quiet Hours' again. You can also toggled the feature by right-clicking the Action Centre's taskbar notification area icon.



10 STAYING INFORMED

The Action Centre is a key part of Windows 10, so now you've mastered it and tweaked it to your personal tastes you can take full advantage of its ability to give you timely information when you need it. As time goes on and more programs are updated to use it, you'll likely find the Action Centre becomes an integral part of your day-to-day computing life.

Create and format sparklines in Excel VBA

Helen Bradley explains how to add, format and delete sparklines using Excel macros.

Sparklines are small in-cell charts that were introduced in Excel 2010. They allow you to compare data in a visual way without creating full size charts to do so. This month we'll show you how to work with sparklines using VBA code.

Our solution uses some Australian Bureau of Statistics data for CPI values but you can use data of your choice. We are assuming that the data for the sparklines starts in cell D3 and that it spreads over a number of columns to the right and rows below. Column C will contain the sparklines.

This is the code to automatically create, format and delete sparklines:

```
  Option Explicit
  Public mysparkers As
SparklineGroup

  Sub addSparklines()
  Dim sparkersRange,
sparkersDataRange As Range
  Dim LastRow, LastColumn As
Long
  LastRow = ActiveWorkbook.
ActiveSheet.Range("a1").
CurrentRegion.Rows.Count
  LastColumn = ActiveWorkbook.
ActiveSheet.Range("a1").
CurrentRegion.Columns.Count
  Set sparkersRange =
Range("c3", Cells(LastRow, 3))
  Set sparkersDataRange =
Range("d3", Cells(LastRow,
LastColumn).Address())
  Set mysparkers =
sparkersRange.SparklineGroups.
Add(Type:=xlSparkLine,
SourceData:=sparkersDataRange.
Address)
  mysparkers.SeriesColor.
ThemeColor = 5
  mysparkers.Axes.Vertical.
MaxScaleType =
xlSparkScaleGroup
  mysparkers.Axes.Vertical.
MinScaleType =
xlSparkScaleGroup
      End Sub

  Sub deleteSparklines()
   Dim rng As Range
   On Error Resume Next
   Set rng = ActiveWorkbook.
ActiveSheet.UsedRange
              For Each
mysparkers In rng.
SparklineGroups
                  mysparkers.
Delete
              Next mysparkers
  End Sub

  Sub flipSparklines()
   Dim rng As Range
   On Error Resume Next
   Set rng = ActiveWorkbook.
ActiveSheet.UsedRange
              For Each
mysparkers In rng.
SparklineGroups
                  If
mysparkers.Type =
xlSparkColumn Then
                  mysparkers.
Type = xlSparkLine
                  Else:
mysparkers.Type =
xlSparkColumn
                  End If
              Next mysparkers
End Sub
```

The first procedure calculates the last row and column when it runs so the macro will work if the data grows or shrinks. The sparklines are created as lines (not columns) and both minimum and maximum vertical axis are configured the same for all the sparklines.

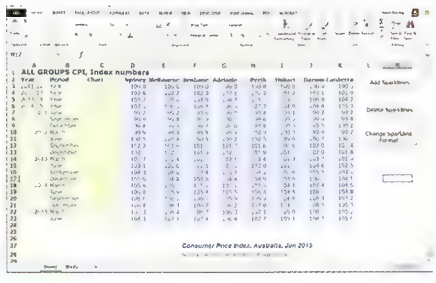
The code to delete the sparklines uses the SparklinesGroups object to process all the sparklines in the worksheet and to remove them. The flipSparklines code toggles the sparklines between displaying as lines and as columns. The deleteSparklines and flipSparklines code can be used with sparklines that you create using our code or with any worksheet which contains sparkline charts.

You can adapt this macro to your own needs. So, if your data has a totals column you can adjust the LastColumn value accordingly to omit this data from the sparklines.

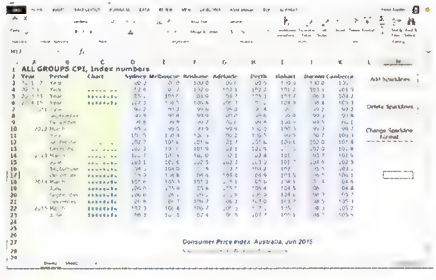
We have chosen to add buttons to the worksheet using the Form tools on the Developer tab and to assign the macros to these buttons making it easier to run the macros when needed.

Creating sparklines using a macro like this ensures that they are created as a sparkline group. As a group they will be adjusted, formatted and deleted as a group. Creating them as a group and configuring the axes to be the same for all, also ensures more accurate data comparison.

STEP 1
This is our code to create the sparklines, delete them and alter their look.



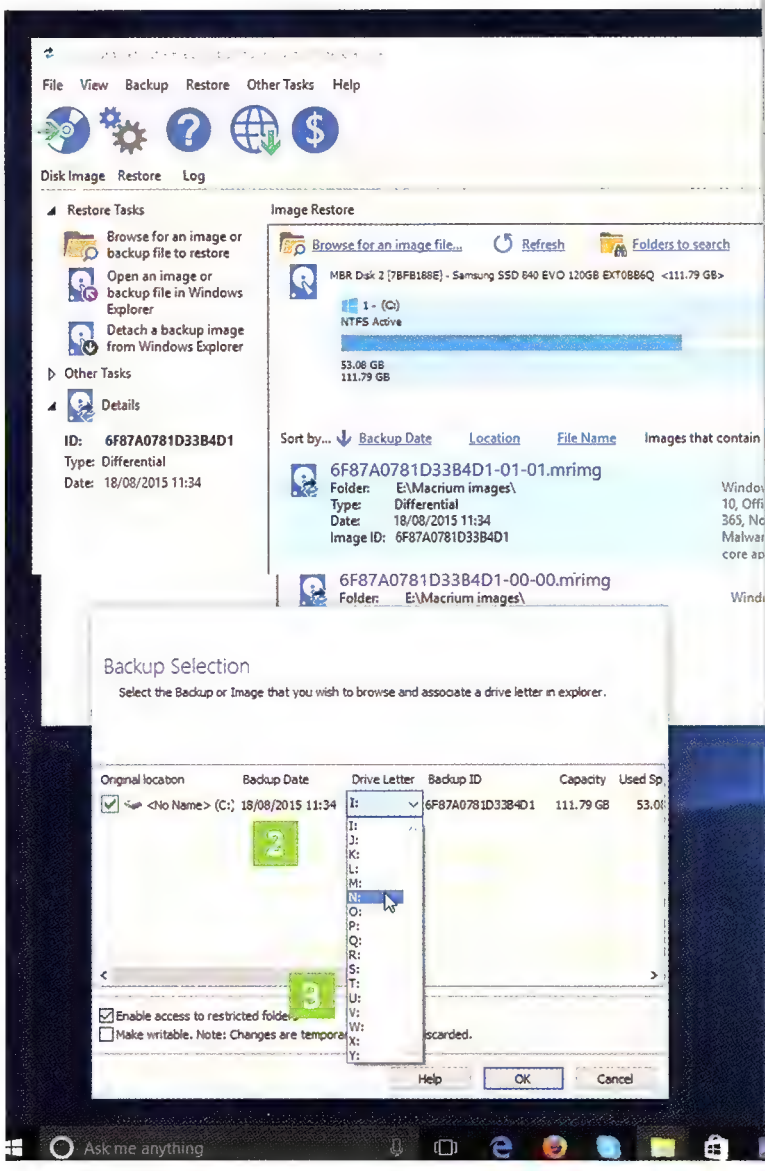
STEP 2
Clicking 'Add Sparklines' will add sparklines charts to column C of the workbook.



STEP 3
Clicking to 'Change the Sparkline Format' changes the sparklines from lines to columns and vice versa.

Make a fail-safe backup

To avoid disaster, take regular backups of your entire Windows drive with Macrium Reflect Free. Nick Peers breaks it down for you.

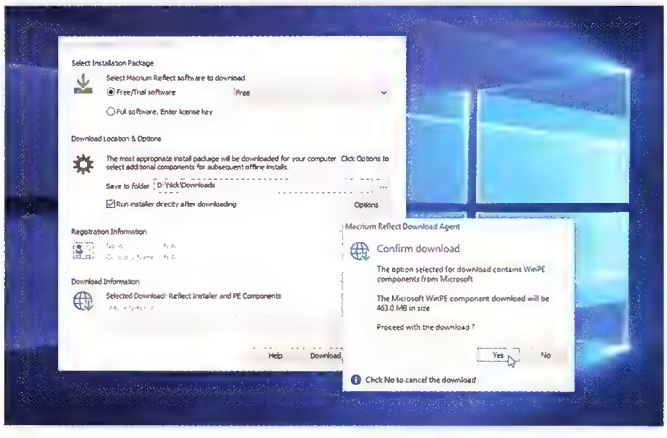


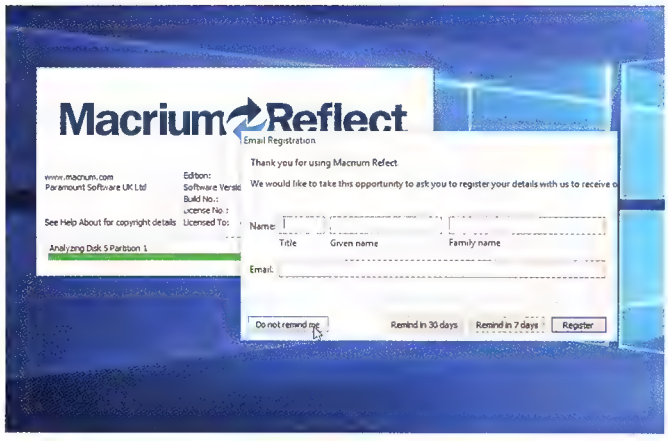
Drive images are an essential part of your backup plan because they take an exact copy of your entire hard drive – the problem with the Windows Backup tool is that each drive image it takes is a completely new copy of your drive, taking time to complete and eating up precious hard-drive space in the process.

Macrium Reflect Free offers a number of advantages over Windows Backup, most notably support for differential backups. These only record the changes made since the last full backup was taken, which not only speeds up the backup process, but also leaves more free space on your backup drive too.

In this tutorial we'll show you how to set up Reflect Free to back up your drive, then – if the worst happens – restore the latest backup so you can quickly recover from a crash or simply undo your most recent changes.

Back up and restore using Reflect



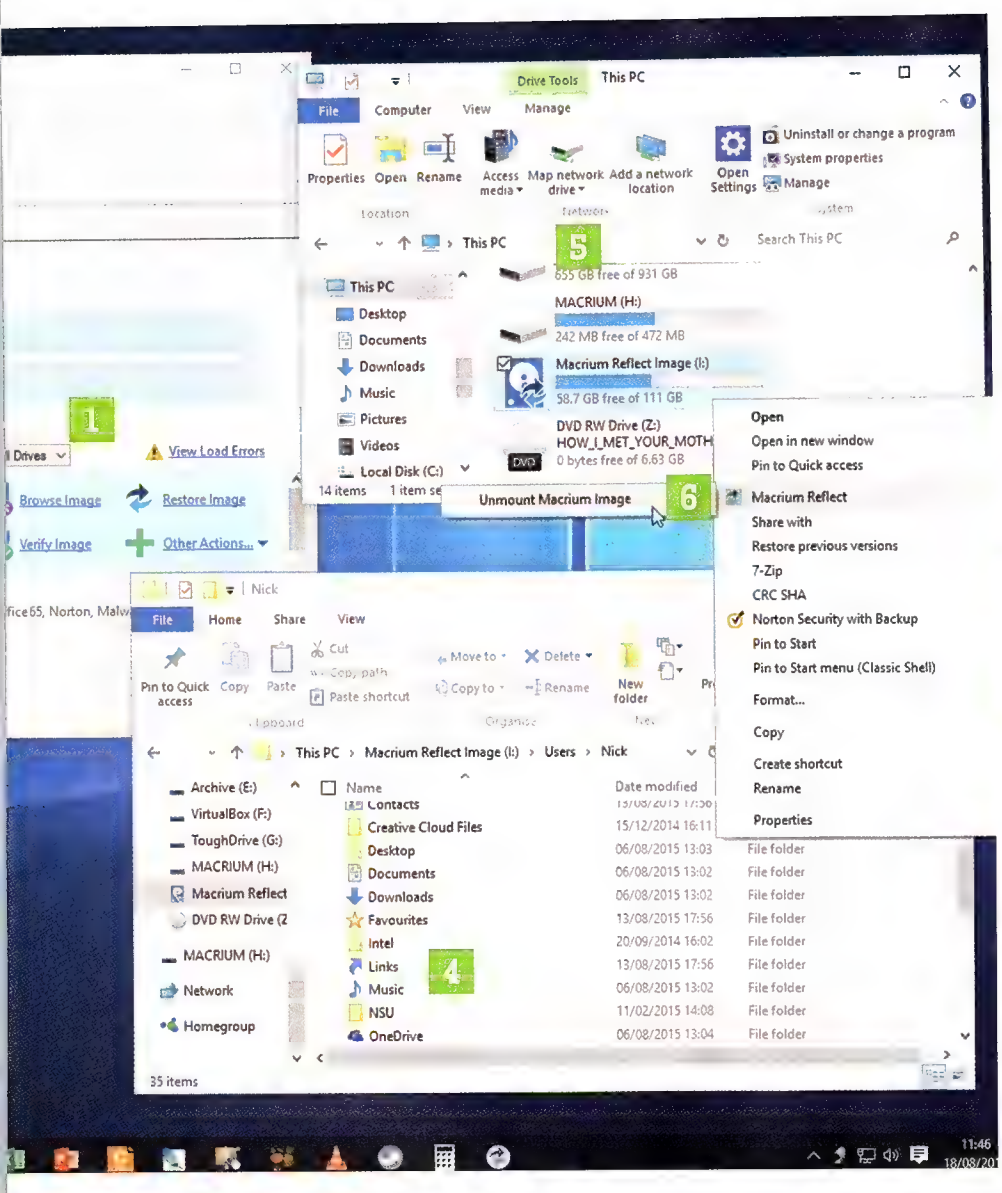


1 DOWNLOAD MACRIUM REFLECT

Download the program installer (ReflectDL.exe) from **macrium.com/reflectfree.aspx** by clicking the green 'Download Now' link. Once saved, double-click the file to open the Download Agent. Make sure 'Free' is selected, and that the 'Selected Download' reads 'Reflect Installer and PE Components' — if not, click 'Options' to select it. Click 'Download' followed by 'Yes'.

2 COMPLETE INSTALLATION

Once the files have downloaded, click 'Next' and follow the setup wizard. If you don't want to, you don't need to register to use the product. After, click 'Finish launch Reflect' from the Start menu by typing `reflect` into the search box. When prompted again to register, simply click 'Do not remind me' to go to the main screen.



Restoring individual files from Reflect backups

1 SELECT IMAGE
Switch to the 'Restore' tab in 'Reflect', then locate the image you wish to recover files from. Click the 'Browse image' link.

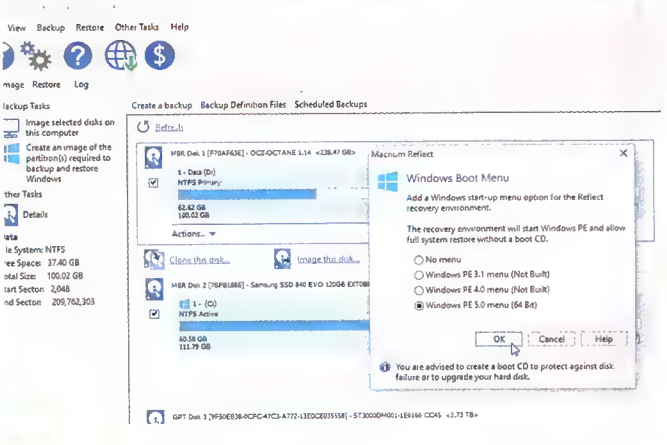
2 CHOOSE DRIVE(S)
Tick the drive or drives you wish to access. Make a note of its drive letter, or click to choose your own.

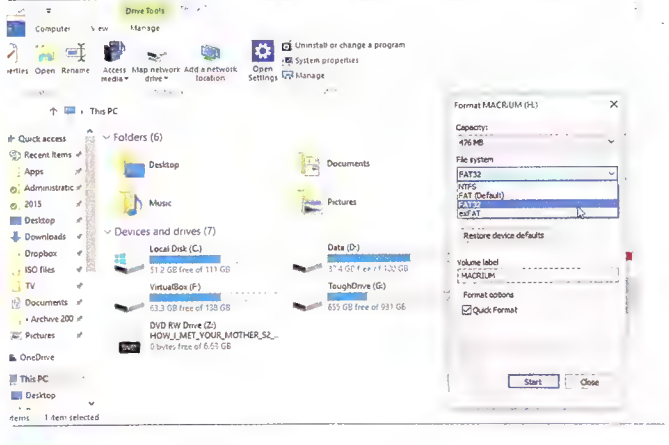
3 FULL ACCESS
To gain full access to the drive, make sure you tick the 'Enable access to restricted folders' box.

4 ACCESS FILES
Once mounted, your image can be accessed like any other drive – just locate your files and copy them off.

5 IDENTIFY DRIVES
Mounted images can be easily identified in File Explorer by the Reflect icon that's assigned to them.

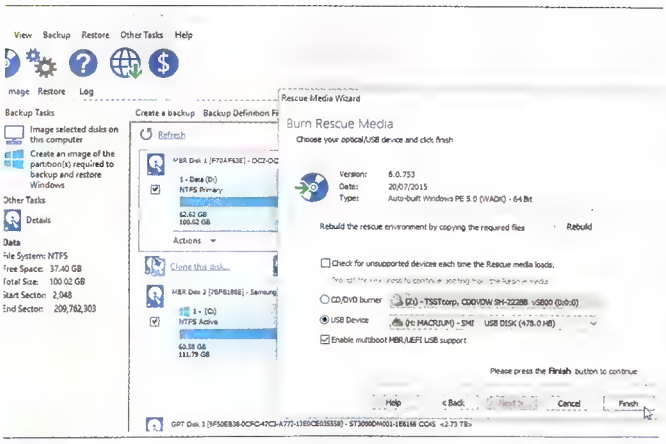
6 UNMOUNT DRIVE
When you're finished recovering data, right-click the drive and choose 'Macrium Reflect > Unmount Macrium Image'.


View
Backup
Restore
Other Tasks
Help
Create a backup
Backup Definition Files
Scheduled Backups
Macrium Reflect
Windows Boot Menu
Add a Windows start-up menu option for the Reflect recovery environment.
The recovery environment will start Windows PE and allow full system restore without a boot CD.
No menu
Windows PE 3.1 menu (Not Built)
Windows PE 4.0 menu (Not Built)
Windows PE 5.0 menu (64 Bit)
OK
Cancel
Help
You are advised to create a boot CD to protect against disk failure or to upgrade your hard disk.



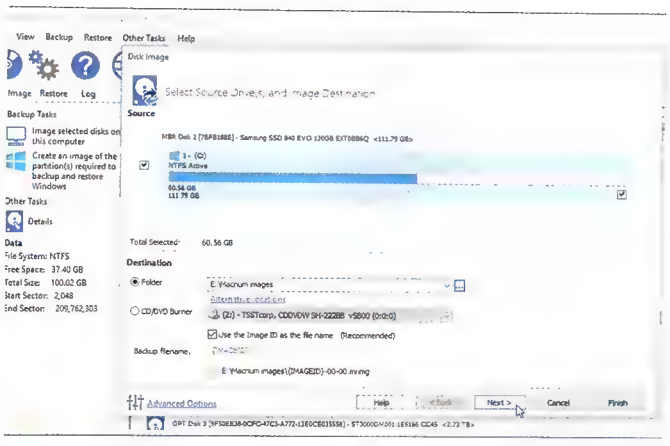
3 SET UP RESCUE OPTIONS
The first step is to provide recovery options allowing you to restore your backup should Windows fail to load. Open the 'Other Tasks' menu. To add an option to launch 'Reflect' when your PC starts, choose 'Add Recovery Boot Menu Option…' and follow the prompts. Select 'Windows PE 5.0' if you're running Windows 8 or later; 'Windows PE 3.1' for Windows 7 or earlier. Click 'OK'.

4 PREPARE BOOT MEDIA
You should also create a rescue disc for added insurance against hard drive failure. You'll need a blank CD or DVD, or a small (512MB or larger) USB flash drive. The flash drive needs to be blank and formatted correctly. Plug it in, open File Explorer, right-click the drive and choose Format. Select 'FAT32' under 'File System' and click 'Start'.



5 CREATE RESCUE DISC

Now select 'Other Tasks > Create Rescue Media' in 'Reflect'. Verify the PE version is correct (see step three) and click 'Change PE Version' if necessary. Click 'OK' followed by 'Next', verify core drivers (network and disk primarily) are selected and click 'Next'. Choose your media (CD or USB), tick 'Enable multiboot…' if using USB and click 'Finish'.

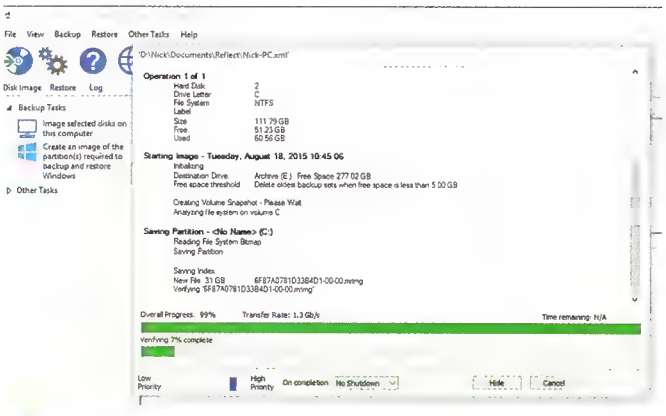


6 TAKE FIRST BACKUP

Next, click 'Create an image of the partition(s) required to backup and restore Windows' under 'Backup Tasks'. Click the '…' button to select a dedicated folder on your backup drive. Click 'Advanced Options', select 'Auto Verify Image' and tick the 'Verify image…' box. Use 'Comments' to help identify the backup. Click 'OK' followed by 'Next'.

7 CHOOSE BACKUP TYPE

The default backup settings will use a mixture of full and differential backups to give you a choice of restore options going forward. Click 'Add Schedule > Full' — by default, a monthly schedule is set, so click 'OK' (or tweak if necessary). Now click 'Add Schedule > Differential' to create a weekly schedule. Click 'Next', review your settings and click 'Finish'.

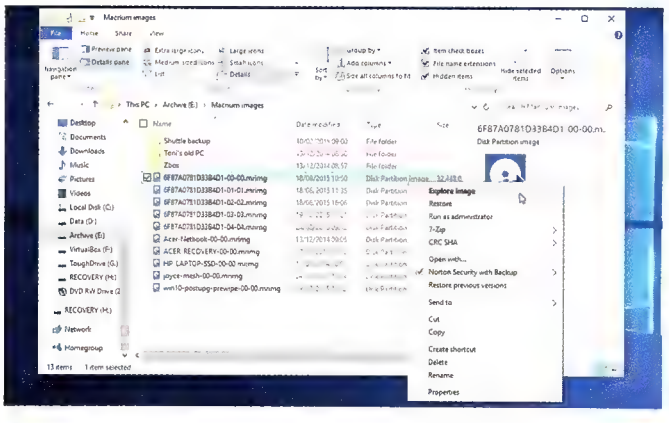


8 RUN BACKUP

Give your backup a suitable name, make sure both boxes are ticked and click 'OK'. You'll be prompted to enter your account password to allow the schedule to be set, so Reflect can back up automatically in the background. Do so, then click 'OK' and wait while the first backup is taken. Once complete, it will verify the image isn't corrupt – your PC is now protected!

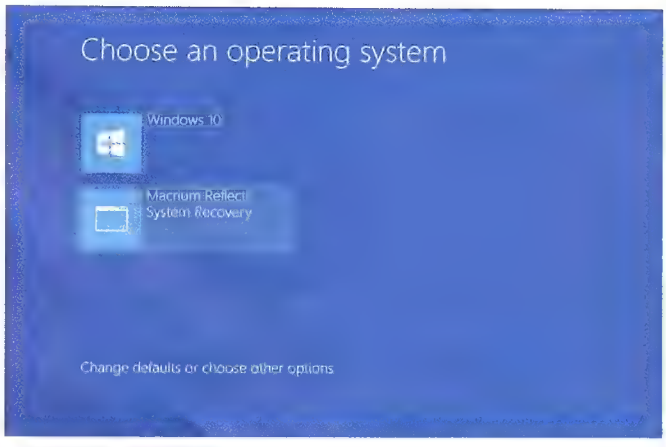
9 UPDATE YOUR BACKUP

Reflect will now update your backup to the schedule you chose earlier, but you can also create backups manually whenever you want — just before installing a major update, for example. To do so, switch to the 'Backup Definition Files' tab, right-click your backup XML file and choose 'Run Now > Prompt'. Choose 'Full' or 'Differential,' add a comment, then click 'Finish'.



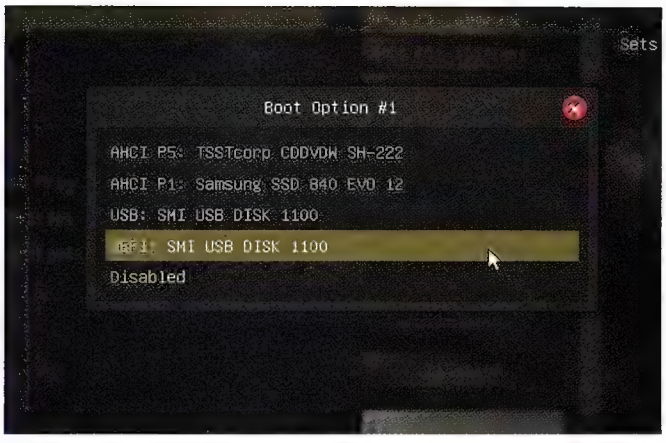
10 RESTORE OPTIONS

There are two basic options when it comes to restoring data. To recover individual files from your backup, mount the image file as a virtual drive in Windows following the annotation on the previous page, then simply copy the files you want from here back to your hard drive. If you need to roll back your entire Windows system, however, read on…



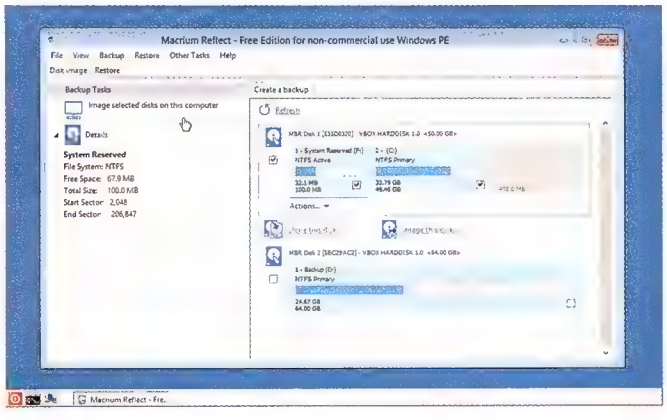
11 RESTORE YOUR BACKUP

While it's possible to start the restore process from within Windows (switch to the Restore tab), it's better to restore a system image from outside of Windows in the recovery environment. If you added the recovery boot menu option in step three, restart your PC — when the boot menu appears, choose 'Macrium Reflect System Recovery' and jump to step 13.



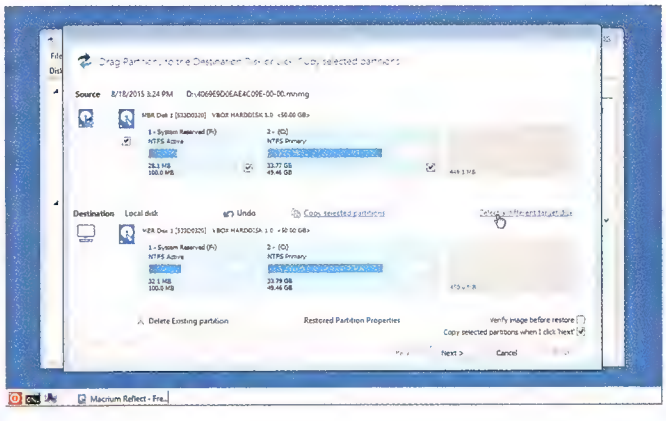
12 USE THE BOOT MEDIA

If you can't boot to the recovery environment, then use your rescue disc or USB drive. Insert it prior to starting up your PC then look for a message that prompts you to access the boot menu — typically it's pressing a key like F11. Use the cursor keys to select your drive from the list of available options and hit Enter to load from it.



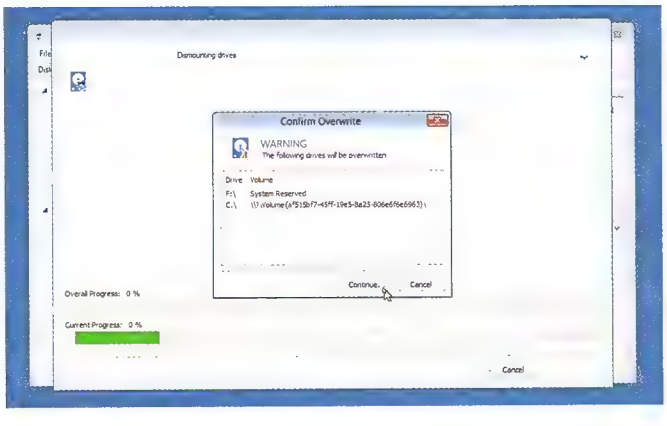
13 IMAGE CURRENT STATE

Restoring a drive image basically wipes out everything that was on the drive before — if there's data you need to protect, take a fresh drive image. Switch to the 'Disk Image' tab, then untick everything except the drive you plan to restore (typically C:). Click 'Image selected disks on this computer' and follow the prompts to back up to your backup drive.



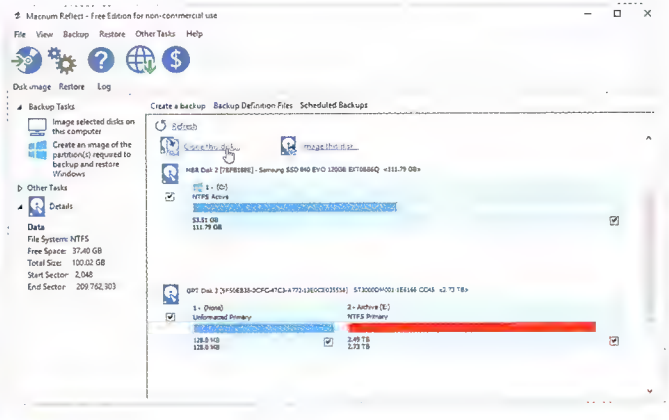
14 SELECT BACKUP TO RESTORE

Once done, switch back to the 'Restore' tab. If your list of images isn't present, click 'Browse for an image file…' to locate it manually on your backup drive. Click 'Restore Image' and Reflect should attempt to automatically select the correct disk; if not, click 'Select a different target disk' to manually choose it.



15 REVIEW AND RESTORE

Click Next to review your proposed changes. Click 'Advanced Options' for additional options such as verifying the image prior to restoring it — note that the 'Rapid Delta Restore' option isn't available in the free edition. Once done, click 'Finish', review the warning and click 'Continue…' Your backup will be restored — choose 'File > Exit' to reboot when done.


Macrium Reflect - Free Edition for non-commercial use
File View Backup Restore Other Tasks Help
Disk image Restore Log
Backup Tasks
Create a backup Backup Definition Files Scheduled Backups
Refresh
Image selected disks on this computer
Create an image of the partition(s) required to backup and restore Windows
Other Tasks
Details
Data
File System: NTFS
Free Space: 37.40 GB
Total Size: 100.02 GB
Start Sector: 2,048
End Sector: 209,762,303

16 YOUR PC, PROTECTED

Congratulations. You now have a fail-safe — and automatically updated — backup that will help minimise data loss and disruption going forward. No more hours lost to reinstalling Windows from scratch and setting up your PC again after a crash; now the most you'll lose is a week's work — or even less if you pair Reflect with Windows' File History tool.

WHAT WOULD STEVE DO?

AT ALL GOOD NEWSAGENTS!

- THE STORY OF MINECRAFT
- MIND-BLOWING BUILDS
- NEW BIOMES AND ENVIRONMENTS
- 31 CHILLING HALLOWEEN MODS
- FOUR PULL-OUT POSTERS

AND MUCH MORE!

ISSUE 04
OUT NOW
ONLY $8.95!

disc contents

» OUR SELECTION OF EXCLUSIVE FULL-VERSION PROGRAMS

ISSUE 422 DECEMBER 2015

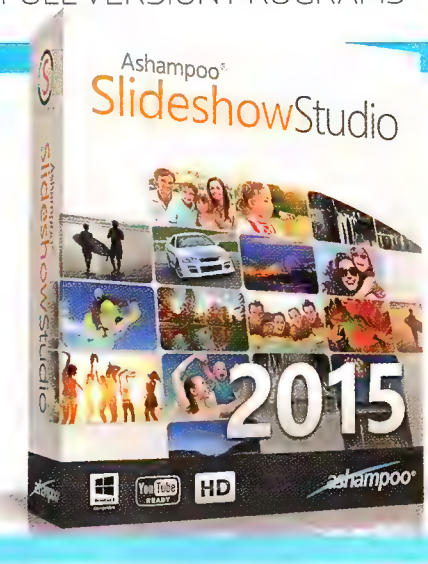
MAKE YOUR MEMORIES SING

Create beautiful presentations with Ashampoo Slideshow Studio

FULL VERSION WORTH $39.99

Your photos have a story — tell it with Ashampoo Slideshow Studio HD 3. Turn your photos into a cinematic experience with smooth zooms and tracking shots, apply fully animated slide transitions and create vibrant full HD videos with ease.

DOWNLOAD LINK: WWW.ASHAMPOO.COM/LPA/APCMAGAZINE



Toolkit #1: 5 Great Safety Tools for Windows

A specially-curated selection of apps to help secure your Windows PC, including:

LASTPASS
With LastPass, you can generate the most secure passwords possible and store them in an online vault to ensure you're never locked out of anything.

AVG FREE ANTIVIRUS
You could pay up to $100 for a security suite, but AVG performs just as well on industry standard tests.

WINPATROL
This program monitors vital folders on your PC for signs of viruses and spyware, let you know if changes are made to critical areas so you can take action.

SOPHOS VIRUS REMOVAL TOOL
If a virus has made its way through your usual defences, it's probably disabled your antivirus software. That's where this tool comes in.

ISPY CONNECT
ISpy Connect lets you use a webcam it as a security camera, streaming sound and video over the internet and emailing you snapshots of any suspicious activity.

HEAD TO WWW.APCMAG.COM/EXCLUSIVES TO DOWNLOAD THE APPS FROM THIS TOOLKIT.

Toolkit #2: 5 Essential Media Apps

This special selection of media apps are favourites of the *APC* staff.

DARKWAVE STUDIO
Darkwave Studio is a free digital audio workstation that supports multi-track hard disk recording, and VST plug-ins for effects and sounds.

FOOBAR2000
If you want something super-lightweight to play your music, there's nothing better than Foobar2000.

GIMP
This free alternative to Adobe Photoshop has the image-editing power you need to make your photos look incredible.

RENAME MASTER
Use Rename Master to quickly retitle batches of photos and other media files.

AUDIOGRABBER
Turns your CDs into MP3 files, outputting fully labelled and tagged files at your specified choice of bitrate.

HEAD TO WWW.APCMAG.COM/EXCLUSIVES TO DOWNLOAD THE APPS FROM THIS TOOLKIT.

NO DISC FOR NEW ZEALAND READERS?

Due to a New Zealand legal requirement that all physically-distributed video games (including indie titles and demos) be rated by the Classification board, we're sadly no longer able to offer our cover disc in New Zealand. However, so our loyal NZ readers don't miss out, we've created a special download page where you can access the exclusive software each month. You'll find it at **www.apcmag.com/exclusives**. While we've created this download page for New Zealand readers, it's also open to all of our Australian and tablet-edition readers too. All you need are the links and zip passwords printed above to be able to download and extract these exclusive full-version apps.

SYSTEM REQUIREMENTS

- A DVD-ROM reader or burner.
- The *APC* disc is designed for use with up-to-date browsers (for example, Internet Explorer, Chrome, Firefox).
- The interface included on the *APC* disc requires a JavaScript-enabled browser.
- An internet connection may be required for online registration of software before use.
- The software packages on the *APC* disc have different system requirements. Software is included on the disc for Windows Vista, 7 and 8.

BEFORE INSTALLING

- Check the disc using a virus scanner complete with the latest antivirus data updates. The disc was checked before burning, but new viruses are being discovered all the time.
- Back up any important system and data files. It is not recommended that the software contained on these discs be installed on production machines.
- If you have any questions regarding the use of the *APC* disc, click the 'Help' button at the top of the screen.

USING THE DISC

- Insert the disc into a CD/DVD-ROM reader or burner and your web browser should automatically load the interface. If not, launch your web browser and load the default.html file from the root directory of the disc.

HELP

- If you have any problems with the *APC* disc, please visit **www.apcmag.com/disc**
- *APC* provides no technical support for this disc or any software provided on it.

NO DISC?

Please note the free disc is not included with NZ copies, digital editions or bundled promotional copies of *APC*.

DISCLAIMER Future Publishing is not the licensor of the software and documentation on the enclosed disc (the 'software'). Rather, Future is merely a distributor of the software, and your use of the software is subject to any accompanying third party licence terms. You must carefully read and comply with any such third party licence terms, together with all instructions and README files that come with the software. Accordingly, to the maximum extent permitted by law, all software is provided by Future 'as is' and without warranty either express or implied, and Future will not be liable for any damage that you may incur as a result of using the enclosed disc. You should back up any important system and data files before using the enclosed disc. We recommend that you do not use the enclosed disc on a production machine. Nothing in this disclaimer excludes any warranty that may be implied by statute, which may include the Trade Practices Act. Notwithstanding the foregoing, if the enclosed disc is faulty or damaged, we will replace them for you. While we have taken all reasonable steps to check the enclosed disc for viruses, we cannot guarantee that it is free from viruses or other harmful code and you should check each disc using a virus scanner complete with the latest antivirus updates before use.

Unlocking El Capitan's not-quite-Siri

Matthew JC. Powell shows you how to use El Capitan's enhanced speech recognition capabilities.

If you're a Mac user who's also got an iPhone or iPad, you may be a bit frustrated that Apple has not yet brought the powerful Siri speech-activated personal assistant to its non-mobile platforms. It's especially frustrating when you see Windows 10 users showing off what Cortana can do. (Windows users shouldn't be able to show off to Mac users – that's just wrong!)

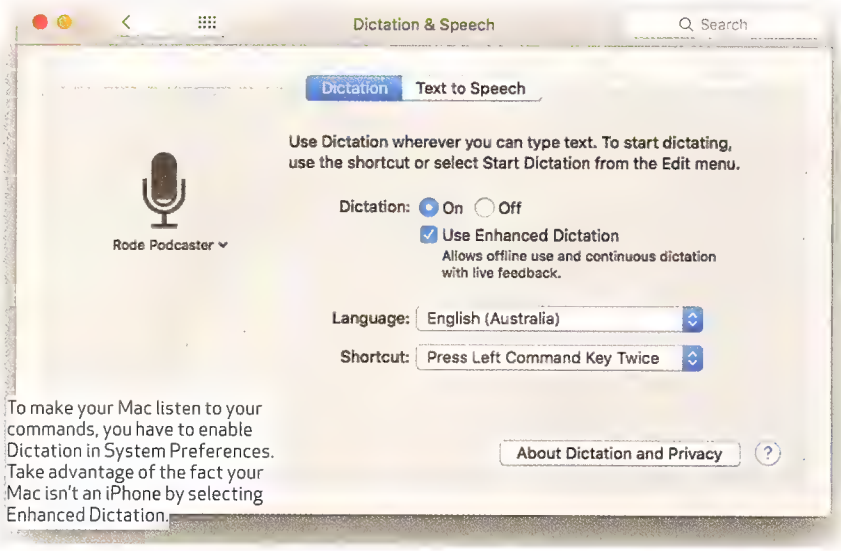
Thankfully, El Capitan has built upon the already improved speech-recognition capabilities of Yosemite, so the day when proper Siri-like functionality arrives on Mac seems just that little bit closer with a smart tweak or two.

The first thing you'll want to do is open System Preferences and click on the Dictation & Speech pane. Next, click the radio button to turn Dictation on, and then click the box for Use Enhanced Dictation. The latter will initiate a download of various stuff that the Mac needs in order to be able to process speech recognition locally, rather than sending everything out over the network for processing to be done on Apple's servers, the way it is with Siri. Since your Mac has both the capacity and the processing grunt to do this processing itself (unlike your iPhone, which does not) you might as well use it.

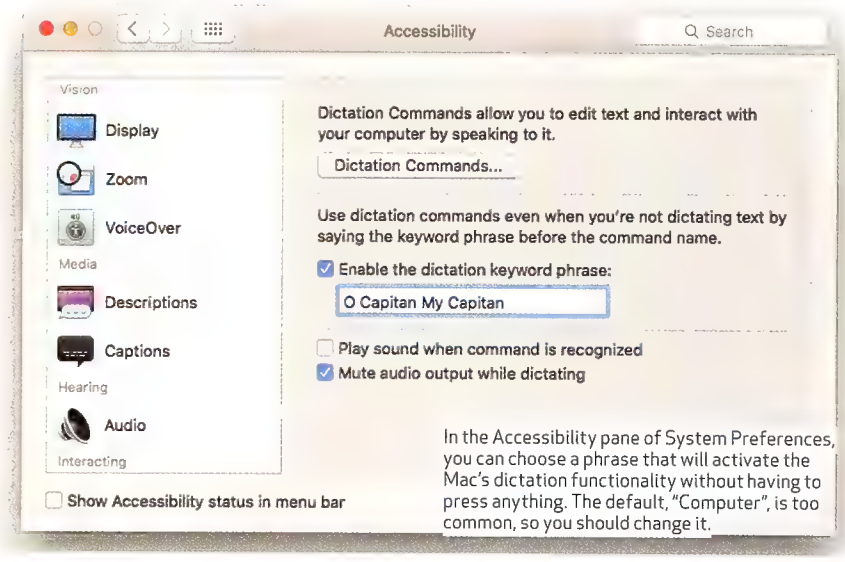
Next, go back out to System Preferences and select the Accessibility pane. Here you'll see that the default trigger for initiating Dictation Commands is the word "Computer". If you're a *Star Trek* fan who does not mind being terminally daggy, you may like to keep it that way. The downside is that "computer" is a fairly common word and the kind of thing you may find yourself saying without intending for your Mac to spring to attention and attempt to follow whatever command comes after.

(If you've ever had your iPhone or iPad go stupid on you because it heard something that sounded a bit like "Hey Siri" you'll understand what we're getting at here.)

For that reason, you should change this to something a little less common and unlikely to be said accidentally. We've used "O Capitan My Capitan" because we're *Dead Poets Society* fans who don't mind being terminally daggy.


Dictation & Speech
Search
Dictation
Text to Speech
Use Dictation wherever you can type text. To start dictating, use the shortcut or select Start Dictation from the Edit menu.
Rode Podcaster
Dictation: On Off
Use Enhanced Dictation
Allows offline use and continuous dictation with live feedback.
Language: English (Australia)
Shortcut: Press Left Command Key Twice
About Dictation and Privacy

To make your Mac listen to your commands, you have to enable Dictation in System Preferences. Take advantage of the fact your Mac isn't an iPhone by selecting Enhanced Dictation.

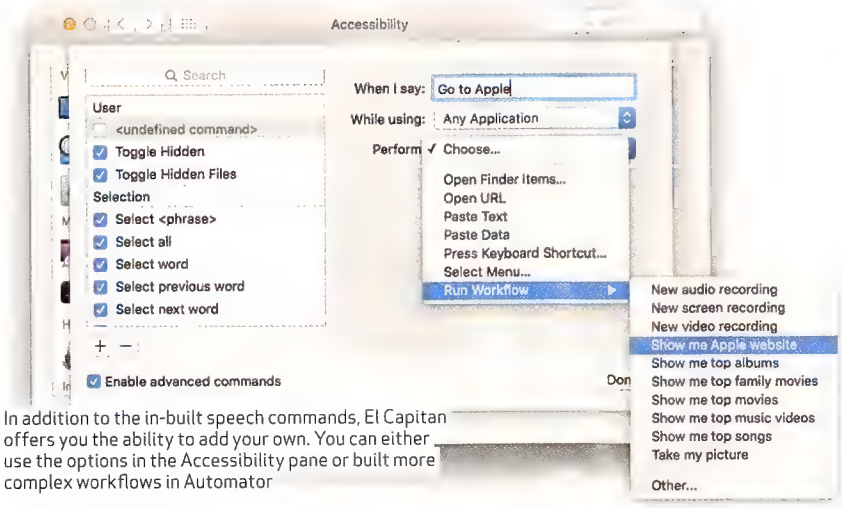


In the Accessibility pane of System Preferences, you can choose a phrase that will activate the Mac's dictation functionality without having to press anything. The default, "Computer", is too common, so you should change it.

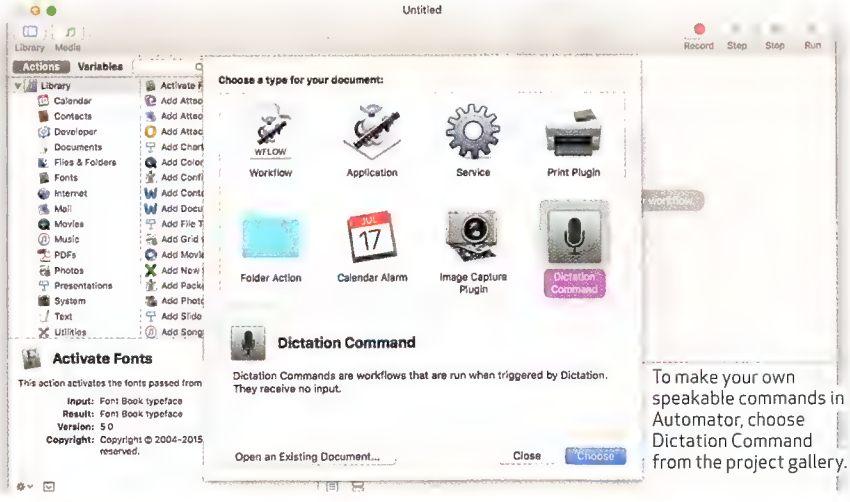
Next, click on "Dictation Commands" to see a list of the various commands you can use speech to activate. A range of them are built in, covering functionality from file handling to navigating the web to selecting and manipulating content within your applications.

You can also use dictation to search Spotlight and, thanks to El Capitan's enhanced natural-language search capabilities in Spotlight, this works rather nicely. For example, say "O Capitan My Capitan, search Spotlight for files created in the last week" and it will parse that correctly. If you get too complex – "O Capitan My Capitan, search Spotlight for files created two weeks ago that are over 100MB" – it can get a little bit lost. This isn't Siri, remember. Not yet.

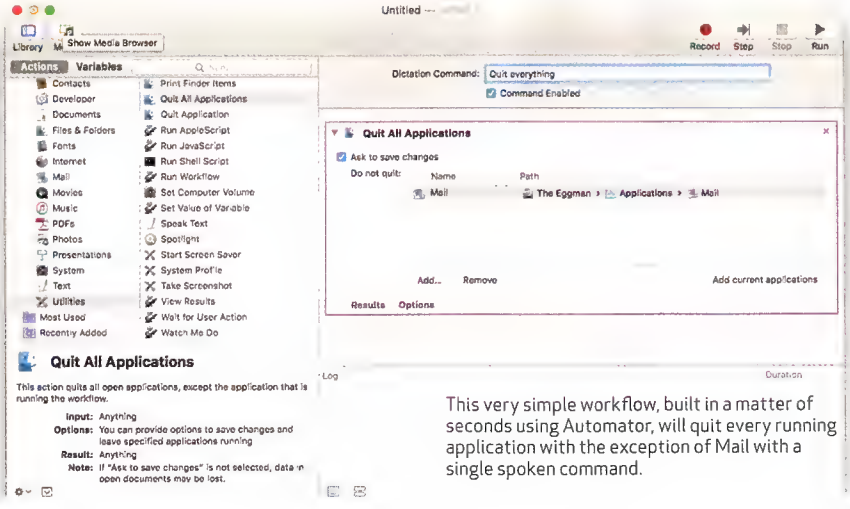
The cool thing that you can do with El Capitan's dictation features that Siri can't match is create your own commands. There are two ways you can do this.



In addition to the in-built speech commands, El Capitan offers you the ability to add your own. You can either use the options in the Accessibility pane or built more complex workflows in Automator



To make your own speakable commands in Automator, choose Dictation Command from the project gallery.



This very simple workflow, built in a matter of seconds using Automator, will quit every running application with the exception of Mail with a single spoken command.

The easiest thing to do is to go back to System Preferences › Accessibility and click on "Dictation Commands" again. In the lower-left corner you'll see a checkbox labelled "Enable advanced commands" – click on that, and another button will appear with + and - symbols. Basically, now you can add or delete commands to the list on in-built ones.

Click on the + symbol, and a dialog appears on the right-hand side, where you can define a phrase to speak, identify the scope of the command (which applications it affects) and define its action from a pre-set list. This is mainly useful if you want custom speech commands for particular keyboard shortcuts or menu items you use often that are not already defined as included commands.

However, you may also notice that at the bottom of the Perform drop-down menu is the option to "Run Workflow".

About the notifications tutorial

Last issue, we described how to use a utility called Terminal Notifier to send yourself messages using the OS X Notification Center, and promised that this issue we would follow up with a way to use Automator to put a nicer graphical interface on the process. Unfortunately, as happens sometimes, the update to OS X El Capitan has altered something in the way Terminal Notifier works, and the steps described in that second tutorial no longer function properly. When we get it working again, we'll bring you that second how-to.

This is where customisable speech recognition really comes into its own – you can define speech commands to run any workflows you've created in Automator, regardless of what type of workflow they happen to be. For instance, if you've created the standalone workflow to toggle visibility of files on and off which we described in an earlier issue, you can activate that workflow using a speech command.

Which brings us to the next way to create custom speech commands – to build them in Automator.

Open Automator, and from the File menu select New... From the project gallery, choose Dictation Command.

Next, create the workflow you want by dragging items from the Library on the left into the workflow window on the right. For example, click on Utilities and then find the command to "Quit All Applications". Drag that over to the workflow window, and in the dialog box at the top, type the text you want to say to activate this workflow – something like "Quit everything" should do. Tick the box to enable the command.

As you can see, there are some other options. Decide whether you want to have the option to save changes to open documents before quitting applications (you probably should), and you can also exclude certain applications from the command if you want – for instance, if you want to be able to quit everything but keep your Mail client open.

When you have the settings as you want them, save the workflow (it's probably wise to give it the same name as the command you want to say to activate it) and Quit Automator. If you go back to the list of Dictation Commands, you'll find your new workflow there and waiting, ready to run at your command.

Create custom vibrations for iPhone

Alan Stonebridge shows you how to find out who's calling you without having to look at your phone.

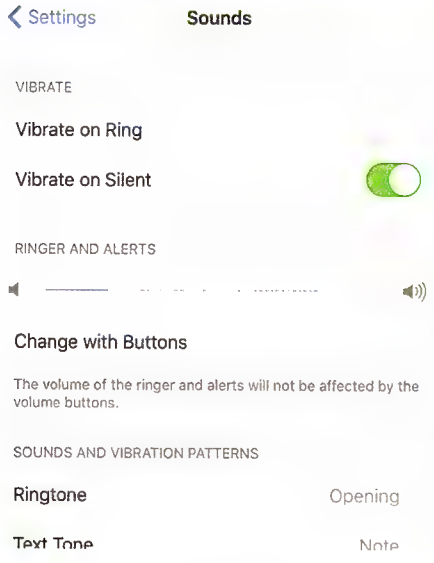
One very useful thing about the Apple Watch is being able to see who is calling without pulling your iPhone out of your pocket. However, your iPhone is already equipped to help you with this. You can complement the ability to assign tones – built into iOS, downloaded from the iTunes Store, or created using GarageBand – with vibration patterns to indicate the type of event the phone wants to draw attention to.

iOS comes with a bunch of predefined vibration patterns, which might be all you need. If you find yourself making extensive use of the feature, you can make your own patterns just by tapping on the screen. Either way, vibrations can be set to occur when the mute switch is engaged, when it's off – or both.

Like sound effects, patterns can be assigned to common events – incoming calls or texts, new email, calendar and reminder alerts and more – but that's not all. If you have specific people whose calls or text messages you really don't want to miss, such as your boss or immediate family members, you don't need an Apple Watch to give you a gentle nudge because your iPhone enables you to assign vibration patterns to individual contacts too.

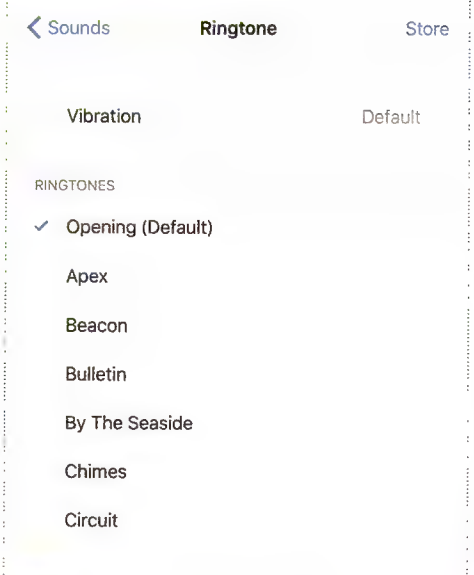
How to:

Assign vibration patterns to events.



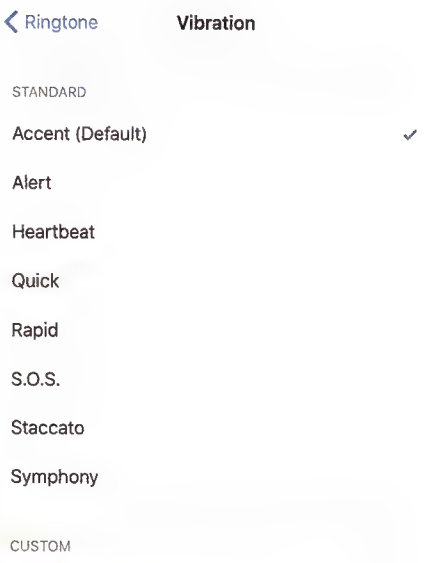
1 SET WHEN TO VIBRATE

Go to 'Settings > Sounds'. At the top of the page, decide whether your iPhone should vibrate whenever a call is received and all sound is turned on (Vibrate on Ring), and if it vibrates when the Mute switch on its side is engaged (Vibrate on Silent); you might leave the latter off if you attend a lot of meetings and don't want even a subtle vibration to seem rude.



2 EVENTS THAT CAN VIBRATE

Further down the Sounds settings page is a list of events that trigger sound effects. What isn't immediately clear is that these items can have a vibration pattern assigned as well as, or instead of, a sound. Tap one and you'll find a Vibration setting; it's above the list of available sounds, so depending on which of those is selected, you might have to scroll up to see it.

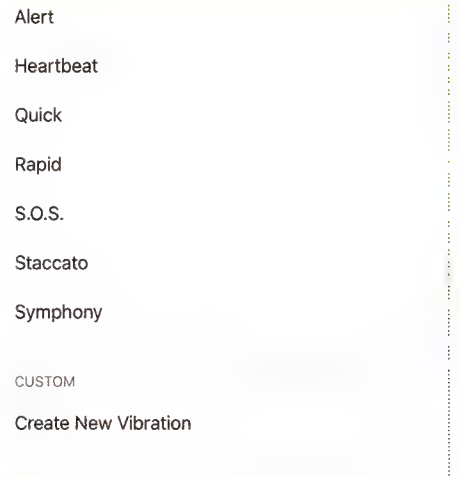


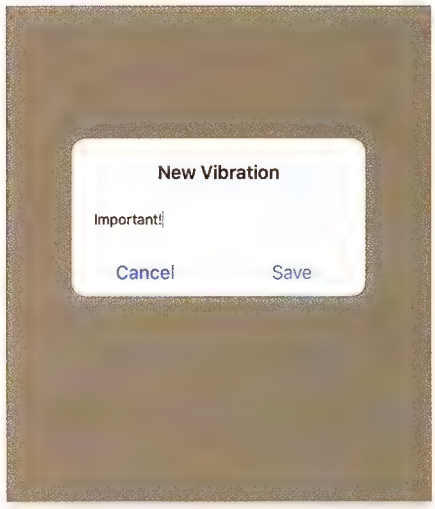
3 ASSIGN A VIBRATION

Tap the Vibration setting and you'll be presented with standard patterns made by Apple. It's set to None by default for the majority of events. Tap the patterns in the list to try them out. You might well find that Apple's own are distinctive enough if you only want to assign vibration patterns to a few events. However, you can be more specific with pattern assignments.

Step-by-step guide

Create your own vibration patterns.





1 TAP OUT A PATTERN

In the same place you can assign one of Apple's own vibration patterns, tap the 'Create New Vibration' option below the list of them. The screen turns largely grey. Tap or hold your finger in that area to build up a pattern. It might take a minute or so of practice to get used to the sensitivity of the interaction. Don't worry if it takes you several attempts to get a good result.

2 CHOOSE YOUR TIMINGS

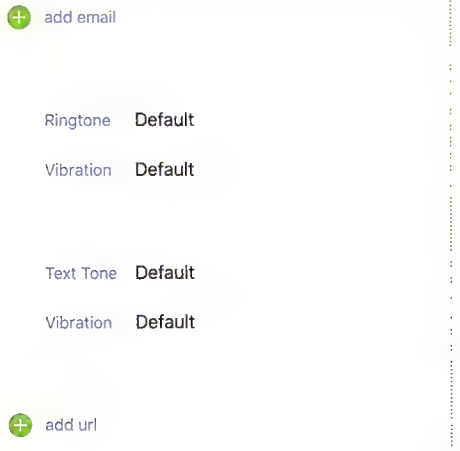
As you lay down a pattern, a blue bar starts to run across the bottom of the screen. There's a maximum length to vibration patterns, but you don't have to fill it. Tap Stop at any time to keep only the duration that has passed — but bear in mind that moments of stillness can be as helpful as vibrations are in telling you what event is taking place.

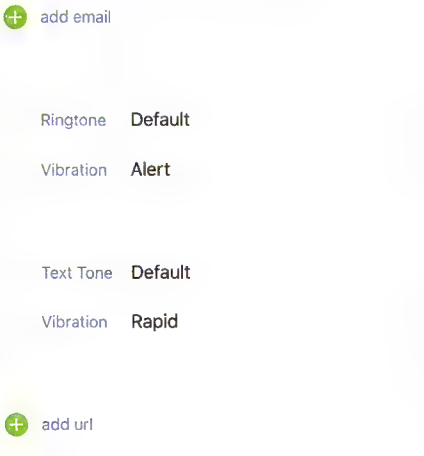
3 SAVE AND ASSIGN IT

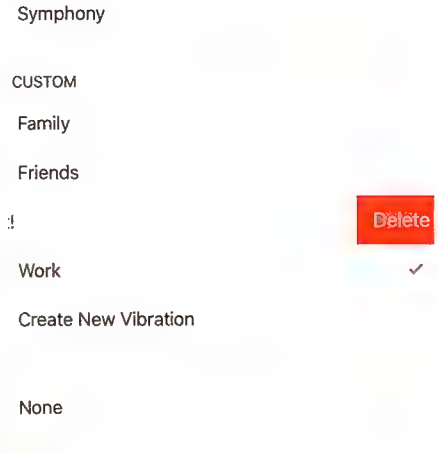
Tap Play to check whether your pattern is good enough, or tap Record to take another stab at it. When you're happy with the result, tap Save, give your pattern a name when prompted, then tap the dialog's Save button. Your pattern will then show up in the list headed Custom, ready to be assigned to events or even to a specific contact.

How to:

Assign vibration patterns to individuals.







1 CHOOSE A CONTACT

Vibration patterns can play in response to more than just broad events. They can be assigned to play when specific people call you or send you a text message. Open the Contacts app, tap on a contact's name to see their details and then tap Edit. Scroll down the list of data you can set for a person until you come to the Ringtone and Text Tone options.

2 ASSIGN TO CALLS OR TEXTS

Notice that Ringtone and Text Tone each have Vibration settings immediately below them, enabling different pattern assignments to be set for the two events. Tap one of them, then tap either one of Apple's patterns or your own (or you can create a new one from here as well) to assign it to that event for this contact only. Tap Done, then Done again to save your choices.

3 MANAGE CUSTOM PATTERNS

Vibration patterns cannot be assigned using Contacts app in OS X or at iCloud.com, and so there are no shortcuts to assign them to whole groups at once. At the list of custom patterns, you can delete one you no longer want by swiping left on it and tapping Delete. Places where that pattern was used will show as 'Unrecognised Vibration' and use a default one.

Back up a drive in Linux

Nick Peers looks at how to use Logical Volume Management snapshots to provide a quick and easy way to undo unwanted system changes.

One of the most compelling reasons for implementing Logical Volume Management (LVM) on your hard drives is snapshots. If you've ever installed a buggy piece of software and then spent ages trying to undo the damage it's caused, or had to sit back while you take a full backup of your hard drive before embarking on some testing, then snapshots will make your life so much easier.

Snapshots are specially created volumes on your hard drive that help record the state of your root drive at the exact moment the snapshot was taken. From this point on, your drive's blocks are monitored for changes, and these changes are then recorded in the snapshot volume. This means you have a fail-safe backup to call on should the worst happen and your system becomes unstable. Snapshots can also be used in less drastic situation, eg if you decide you don't like the changes you've made, and want to quickly roll your system back to the moment when you originally took the snapshot rather than unpick those changes manually.

Originally, snapshots were read-only, so changes to the blocks on your drive were only written to your root volume after a copy of the original block was made to the snapshot volume, with the exact changes recorded in an exception table. This means that any files you add, change or remove – such as through the installation, update or removal of applications – are effectively protected through the snapshot. If they cause problems on your PC, reverting to the snapshot will undo them and restore it to the state it was in when you took the snapshot.

With the emergence of LVM2, snapshots have become read/write by default, and more versatile as a result. As we reveal later on, you can now use a snapshot volume as a sandbox, allowing you to quickly and easily turn your PC into a test bed without having to mess around with full backups or virtual environments. It works by writing changes to the snapshot instead of your main volume, which makes it even easier to recover your original setup should you subsequently encounter problems. If you subsequently decide to keep your changes, then you simply merge the contents of the snapshot volume into your main partition.

In this tutorial, we'll explore how to use snapshots in Ubuntu, both as a simple backup/restore tool, and as a virtual test bed. We're using the latest version of Ubuntu LTS 14.04.2, so the steps may differ if your setup is different.

GET SNAPSHOT READY

Snapshots only work on drives that have been set up using Logical Volume Management. You'll have been offered this option when you first installed Ubuntu – if you ticked 'Use LVM with the new Ubuntu installation', then you're good to go (skip to the next section). However, if LVM hasn't been set up on your system then you have two options: the first is to format or convert your drive to LVM, while the second involves taking a slightly different approach.

If you want to use snapshots as provided by LVM, your first option – formatting the drive – means you'll need to reinstall Ubuntu from scratch, this time ticking the all-important LVM option during installation. In many cases, this approach won't be practical, so it's good to know that there's a workaround that preserves your existing setup. It's a little clunky in places, and if it goes wrong you'll probably end up losing your installation anyway, so take a full system backup before you begin – try the CloneZilla live option **(clonezilla.org)** if you're stumped for a tool to use. Don't skip this step, if the conversion fails, you'll need to restore your backup and try again.

The quickest and simplest way to perform the conversion to LVM is to make use of a free utility called blocks, which does all the hard work for you. It is a relatively painless process, but

Snapshot volume size

One of the trickiest things to manage with snapshot volumes is their size. If you have a large hard drive, then allocating more than you think you'll ever need is easy enough, but what if you're pressed for space? The problem is, if you allocate too little to your snapshot volume and it fills up with all the changes you subsequently make, the snapshot is rendered invalid and you can't use it — even to restore your system from that point. If you have enough free unused space you can resize the volume before it's full, ensuring it continues to work properly. This can be done manually using Logical Volume Manager by selecting your snapshot volume under 'Logical View' and clicking 'Edit Properties' to extend it.

It's also technically possible to instruct LVM to monitor the volume and when it hits a certain threshold extend the volume automatically. To do this, edit the lvm.conf file:

```
sudo gedit /etc/lvm/lvm.conf
```

Search the file for `snapshot_autoextend_threshold` and change the figure to 80 to have it automatically extend once the drive is 80% full (you can reduce this figure all the way to 50). If you want to change the amount the volume extends by, altering the `snapshot_autoextend_percent` figure (default is 20%). Now save the file, close gedit, and restart to enable the change.

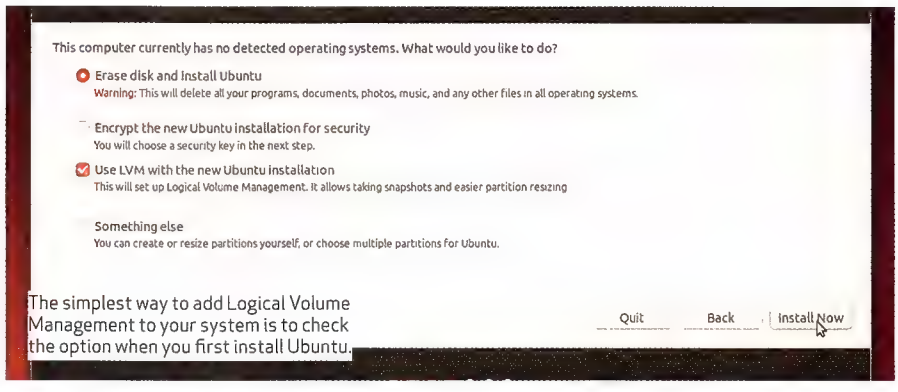
Sadly, at time of writing, the tweak we've covered doesn't appear to work in Ubuntu, but the issue has been reported on Launchpad (see **tinyurl.com/nmu9g6v**).

there's a slight complication in that blocks requires a depreciated version of Python (version 3.3). Don't worry as the 'Convert your drive to LVM' box reveals the exact process to follow. Once the drive has been converted, don't rush to reboot as your install will be unbootable. Don't panic — you need to first repair Grub, and this can be done with the minimum of fuss using the Boot Repair tool. Head to **help.ubuntu.com/community/Boot-Repair** for a complete guide to installing and using it. Simply follow the recommended repair settings, and you should find Ubuntu will boot once again, this time with LVM up and running. Even after this has been done, don't be surprised to see Grub complain about diskfilter writes not being supported. It's a non-critical error — after about five seconds this will clear and your PC will boot normally — it's a confirmed bug in Grub (see **tinyurl.com/nm66vcu**), and a fix should be available sooner rather than later.

If you don't have LVM enabled on your system, and you have no desire to implement it, you can get some of the snapshot functionality using a combination of rsync, diff and Cron with the help of the Back In Time KDE front-end. This enables you to select the folder you wish to back up, then save it to a backup drive or partition. Disk space is minimised by only recording changes, and Back In Time allows you to automatically update snapshots to a set schedule, something you can't do with LVM snapshots. Search your package manager (we're using Ubuntu and Software Center) for 'snapshot' and install the Back In Time (root) version to allow access to all your files.

SET UP YOUR BACKUP VOLUME

LVM snapshots work by creating a volume in an unused portion of your hard drive. This means you'll need to create free space one of two ways: resizing your primary partition to provide enough unused space where these snapshots can reside, or making use of another drive or partition. Wherever you decide to take space from, 10GB should be more than enough, but if space is tight then 2GB (or even less) should be sufficient if your planned changes are minor. If you do find your snapshot volume (or volumes if you store multiple changes) running out of space, you can always allocate more later depending on your circumstances.


This computer currently has no detected operating systems. What would you like to do?
Erase disk and Install Ubuntu
Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.
Encrypt the new Ubuntu installation for security
You will choose a security key in the next step.
Use LVM with the new Ubuntu installation
This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing
Something else
You can create or resize partitions yourself, or choose multiple partitions for Ubuntu.
Quit
Back
Install Now
The simplest way to add Logical Volume Management to your system is to check the option when you first install Ubuntu.

We're going to avoid the terminal by using a free tool called Logical Volume Management, which you can get from the Software Center by searching for LVM. One word of warning: it doesn't behave with RAID drives. (If you fall into this category, check out the Quicktip box, above, for access to the terminal commands you'll need). You can also use the tool to resize your primary partition and allocate the free space from wherever you take it. If you go down this route, you will need to run Logical Volume Management from your live CD, which means installing it from there through the Software Center.

Once installed, launch Logical Volume Management. If you're resizing your root drive, select it under 'Volume Groups > Volume name > Logical View' and choose 'Edit Properties'. Reduce the size of your volume by the amount you need. Click 'OK' and wait while it's resized. Once done, select 'Logical View' where you should now see the Unused Space is visible as part of the volume group. Don't create anything here — this is where your snapshot volume (or volumes) will be stored going forward.

If you make use of a secondary drive, you don't need to give over the entire drive to snapshots — if there's data already on there, use GParted to resize the partition first to free up the space you need. Once done, create a blank, unformatted partition in the free space. You can then switch to Logical Volume Management, where you'll find the new partition under 'Initialised Entities'. Select the partition you wish to use from the list (use its Properties to identify the right one by its size) and click 'Initialise Entity' followed by Yes. Once complete, the drive will now show up under Unallocated Volumes — click 'Add to existing Volume Group', select your existing volume group and click 'Add'. The free space is now available for use.

If you run out of space for snapshots going forward, you can use a combination of both methods — reducing primary partition size or allocating spare storage from other volumes — to increase the amount available to your snapshots.

Your system is now ready to take snapshots — the simplest way to do this is through Logical Volume Management itself. Open it from the launcher, supplying your password when prompted. When the main screen appears, expand Logical View under

Volume Groups, select your root partition and click the 'Create Snapshot' button. If you get an error message about the dm-snapshot module – likely the first time you use it, open a separate terminal window and type `sudo modprobe dm-snapshot`.

Click 'Create Snapshot' again. Give your snapshot volume a suitably descriptive name – testbed, rootsnap or something similar. You can allocate it all the remaining space (click 'Use remaining') or specify an exact size using the LV size box or slider. Leave both Mount boxes unticked and click 'OK'. After a short pause while LVM reloads, you'll see an overview of the new layout. Congratulations, you've just taken your first system snapshot.

This is the point where you need to decide about how you're going to use this snapshot. The simplest method is to use it purely as a fallback, which means you now carry on as normal. Changes are recorded to your main partition, and if anything untoward happens, you can restore the snapshot via the terminal using the following command:

```
sudo lvconvert --merge /dev/<volgroup>/<snapshotname>
```

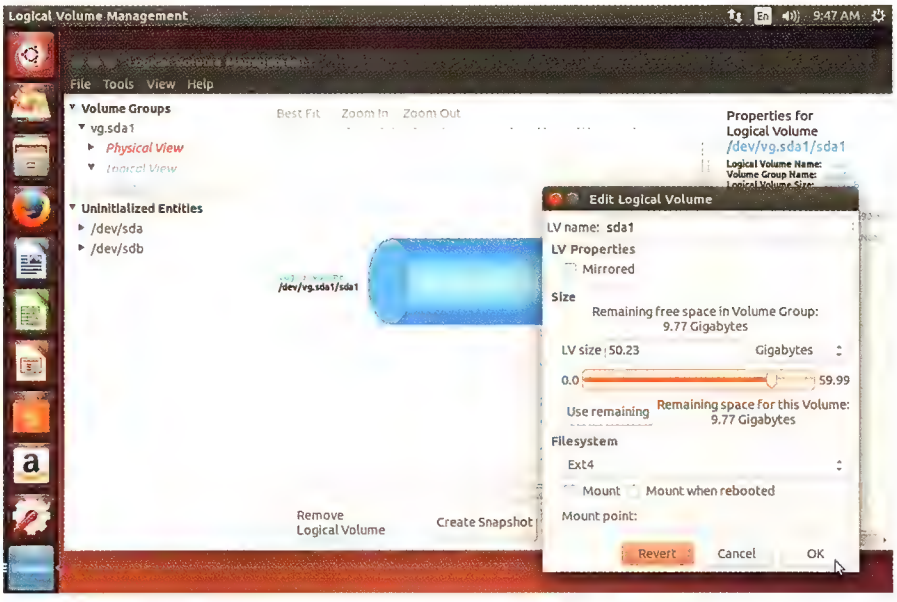
Where `<volgroup>` refers to your LVM's volume group name, and the `<snapshotname>` should be replaced by the name you gave your snapshot volume when you created it – if you're not sure what these are, open Logical Volume Management and select your snapshot under Logical View. You'll see both the snapshot name (Logical Volume Name) and group name (Volume Group Name) listed here.

When you hit Enter, you'll be told it can't be merged over the 'open origin volume', which basically means you need to reboot your system – the snapshot's original files will replace your changes and your root partition effectively rolls back in time to when the snapshot was taken. If your changes have meant you're unable to start up, you can run the command from your live CD.

If you're still unable to start after running the command here, then hold Shift as you boot, then select 'Advanced Options' and choose an older version of the kernel. Once this successfully boots, use software update to bring your installation bang up to date again.

CREATE A VIRTUAL TEST BED

You can also use snapshots in a slightly different way by temporarily mounting the snapshot volume at boot. You'll record changes there instead of to your main partition. If something goes wrong, you can simply reboot to the main partition, and your changes will magically vanish. You can then wipe the snapshot and start again. And if



Convert your drive to LVM

First, boot into Ubuntu and install lvm2 through Software Center. Now open a terminal window and type `sudo nano /etc/fstab` to verify the drives are listed by their UUIDs (if they're not, you'll need to edit the references — use `sudo blkid` to identify them). Once done, type `sudo update-initramfs -u` to rebuild the initramfs image.

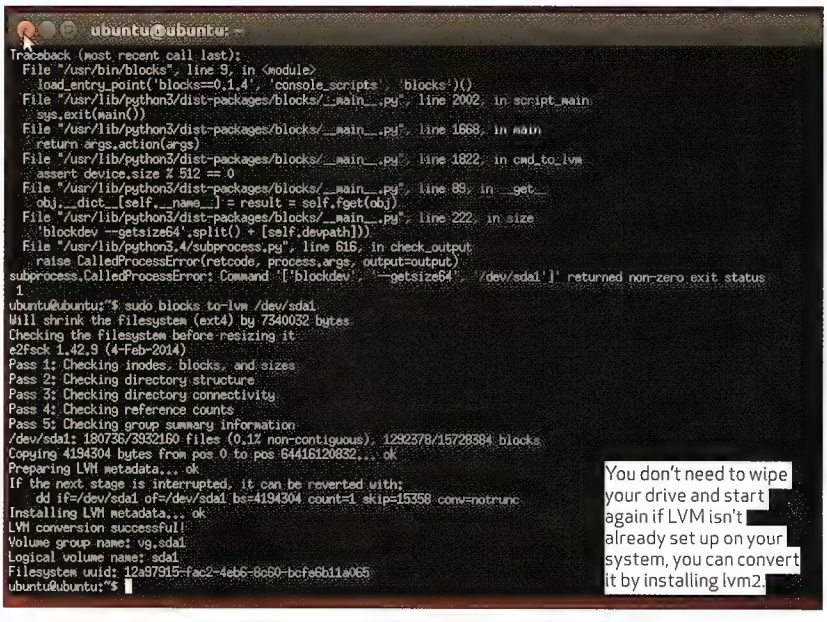
Now, restart and boot from your Ubuntu live CD and open a terminal window and type the following commands:

```
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository ppa:g2p/storage
$ sudo add-apt-repository ppa:fkrull/deadsnakes
$ sudo apt-get update
$ sudo apt-get install python3.3
$ sudo apt-get install python3-blocks bcache-tools
```

Now type the following command into the terminal to perform the actual conversion:

```
blocks to-lvm <device>
```

Replace <device> with the device info — typically dev/sda1 and the drive should now be converted. Make a note of the volume group name (vg.sda1) and logical volume name (sda1) that have been assigned.


ubuntu@ubuntu: ~
Traceback (most recent call last):
File "/usr/bin/blocks", line 9, in <module>
load_entry_point('blocks==0.1.4', 'console_scripts', 'blocks')()
File "/usr/lib/python3/dist-packages/blocks/__main__.py", line 2002, in script_main
sys.exit(main())
File "/usr/lib/python3/dist-packages/blocks/__main__.py", line 1868, in main
return args.action(args)
File "/usr/lib/python3/dist-packages/blocks/__main__.py", line 1822, in cmd_to_lvm
assert device.size % 512 == 0
File "/usr/lib/python3/dist-packages/blocks/__main__.py", line 89, in __get__
obj.__dict__[self.__name__] = result = self.fget(obj)
File "/usr/lib/python3/dist-packages/blocks/__main__.py", line 222, in size
'blockdev --getsize64'.split() + [self.devpath]))
File "/usr/lib/python3.4/subprocess.py", line 616, in check_output
raise CalledProcessError(retcode, process.args, output=output)
subprocess.CalledProcessError: Command '['blockdev', '--getsize64', '/dev/sda1']' returned non-zero exit status 1
ubuntu@ubuntu:~$ sudo blocks to-lvm /dev/sda1
Will shrink the filesystem (ext4) by 7340032 bytes
Checking the filesystem before resizing it
e2fsck 1.42.9 (4-Feb-2014)
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information
/dev/sda1: 180736/3932160 files (0.1% non-contiguous), 1292378/15728384 blocks
Copying 4194304 bytes from pos 0 to pos 64416120832... ok
Preparing LVM metadata... ok
If the next stage is interrupted, it can be reverted with:
dd if=/dev/sda1 of=/dev/sda1 bs=4194304 count=1 skip=15358 conv=notrunc
Installing LVM metadata... ok
LVM conversion successful!
Volume group name: vg.sda1
Logical volume name: sda1
Filesystem uuid: 12a97915-fac2-4eb6-8c60-bcfe6b11a065
ubuntu@ubuntu:~$

You don't need to wipe your drive and start again if LVM isn't already set up on your system, you can convert it by installing lvm2.

things go right, you can merge the contents of your snapshot volume with your main partition to set the changes in stone. The step-by-step guide (below) reveals how to do this.

Note that if you want to continue testing beyond a reboot, you'll need to follow step two of the walkthrough each time to manually instruct Grub to use your snapshot partition. If that becomes tedious, use a tool such as Grub Customizer to create a boot entry for your snapshot volume that you can select each time you start your PC. To do this, open a terminal window and type the following:

```
$ sudo add-apt-repository ppa:danielrichter2007/grub-customizer
$ sudo apt-get update
$ apt-get install grub-customizer
```

Once installed, launch Grub Customizer, select your default entry and click 'Edit'. Press 'Ctrl-a' followed by 'Ctrl-c' on the Source tab to copy the existing text. Click 'OK', then create a new entry. Press 'Ctrl-v' into the Source tab to paste the existing text, then tweak the line beginning `linux` to point to your snapshot partition as instructed in step two of the walkthrough. Click 'OK', and then click on the 'new' name to rename it.

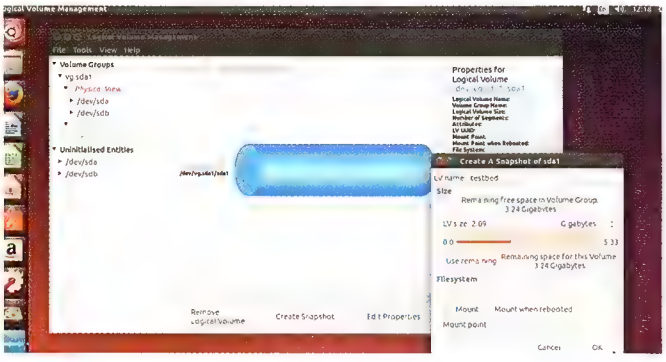
From here on Grub should automatically appear at startup, but if it doesn't, switch to the 'General Settings' tab in Grub Customizer and tick 'show menu' under Visibility, which will allow you to select your snapshot volume as the one to use. Finally, once you're finished with the snapshot, you either have the choice to discard it or merge its changes into your main partition. However, be sure to delete the entry in Grub Customizer.

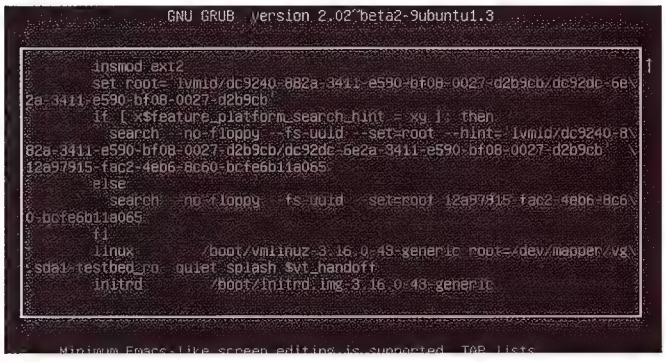
Snapshot volumes normally last as long as you want them to – with one exception (see below). When you've finished with a snapshot volume, you can leave it in place, but once you have no more need of it, you should remove it. The simplest way to do this is through Logical Volume Management – just browse to the snapshot volume under Logical View and click the 'Remove Logical Volume' button you find; you can also remove the volume by selecting 'Logical View' itself – click on the snapshot volume to select it and click 'Remove Selected Logical Volume(s)'.

Review the warning and click 'Yes'. Once a snapshot is removed, the space that it took up reverts to unused space, allowing you to press it back into action for new snapshots.

The only time snapshot volumes are automatically cleaned up is when you merge one back into the main volume using the `lvconvert --merge` command. Once the merge is complete, the snapshot is deleted and the space is automatically marked as unused.

Use snapshots as a virtual test bed



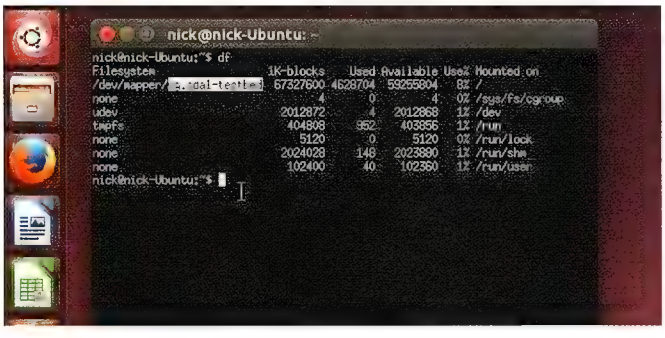


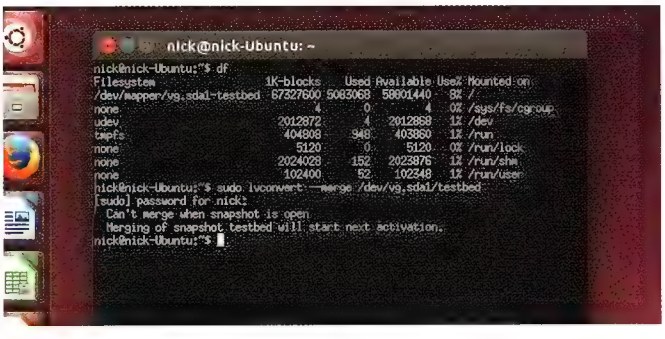
1 TAKE A SNAPSHOT

Create a snapshot as instructed in the main text. Make sure you allocate enough free space to your snapshot partition to accommodate all the changes you plan to test. If unsure, click 'Use remaining' to allocate all available space to the snapshot. Once done, close LVM. Open a terminal window, type `df` and press Enter and make a note of the /dev/mapper/ reference.

2 TEMPORARY BOOT

Restart your PC, holding down Shift as you boot. When the Grub menu appears, press e to access the Grub script text. Use the cursor keys to find the line beginning `linux`, which refers to /dev/mapper/<volgroup>-<snapshot>, where <volgroup>-<volname> matches what you recorded from `df` in the previous step. Change <snapshot> to match the name you gave your snapshot.


nick@nick-Ubuntu: ~
nick@nick-Ubuntu:~$ df
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/mapper/vg_sda1-testbed 67327600 4628704 59255804 8% /
none 4 0 4 0% /sys/fs/cgroup
udev 2012872 4 2012868 1% /dev
tmpfs 404808 952 403856 1% /run
none 5120 0 5120 0% /run/lock
none 2024028 148 2023880 1% /run/shm
none 102400 40 102360 1% /run/user
nick@nick-Ubuntu:~$


nick@nick-Ubuntu: ~
nick@nick-Ubuntu:~$ df
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/mapper/vg_sda1-testbed 67327600 5003068 59001440 8% /
none 4 0 4 0% /sys/fs/cgroup
udev 2012872 4 2012868 1% /dev
tmpfs 404808 948 403860 1% /run
none 5120 0 5120 0% /run/lock
none 2024028 152 2023876 1% /run/shm
none 102400 52 102348 1% /run/user
nick@nick-Ubuntu:~$ sudo lvconvert --merge /dev/vg_sda1/testbed
[sudo] password for nick:
Can't merge when snapshot is open.
Merging of snapshot testbed will start next activation.
nick@nick-Ubuntu:~$

3 USE TEST BED

Once logged in, open terminal again and use `df` to check you're using the snapshot volume rather than your main one. Once verified, you can experiment, secure in the knowledge that all changes are written to your snapshot partition, not your main one. You can reject these changes at any time, simply by rebooting as normal, which will take you back to your main partition.

4 MERGE CHANGES

After you've finished testing, you can keep the changes that you've made by merging your snapshot back to your main volume. Open a terminal window and type the following: `$ sudo lvconvert --merge /dev/<volgroup>/<snapshot>` You'll be told that the merge will happen on the next reboot, so you will need restart to complete the process.

New life for an old PC

Alex Campbell shows how carefullyselected upgrades can give an ageing PC a new round of usefulness, even with older architectures.

THE MISSION

Here at *APC*'s PC Builder Masterclass, we often build new rigs from scratch. We have the option of using just-in, bleeding-edge, nerd-porn-worthy parts, or remixing a fresh build idea from our selection of parts we've already built and reviewed. Either way, builds usually use newer-generation parts. New! Shiny!

This isn't one of those builds. We know that not everyone can, or has, the desire to go out and build a whole new PC every time. In fact, one of the best parts of building a PC is the fact that you can upgrade a system as it begins to show its age. We were digging around in the pile of parts that is the *APC* Lab, and we found a frumpy-looking gem: an LGA1155-based Core i5 budget build from 2013.

Yes, this already less-than-attractive case didn't get any prettier with time. But with a little TLC, we were able to resurrect this rig and get it a little more up to speed.

INHALE

In our original build, the PC had a quad-core Core i5-3350P at its heart. The CPU served the rig well against the competition two years ago, and cost $240 back then. If you can still find it, it now runs about $190. We'd mounted the CPU onto a $90 ECS H77H2-M3 mobo, which is a basic board that gets the job done. The same mobo is $70 today, though finding one won't be easy.

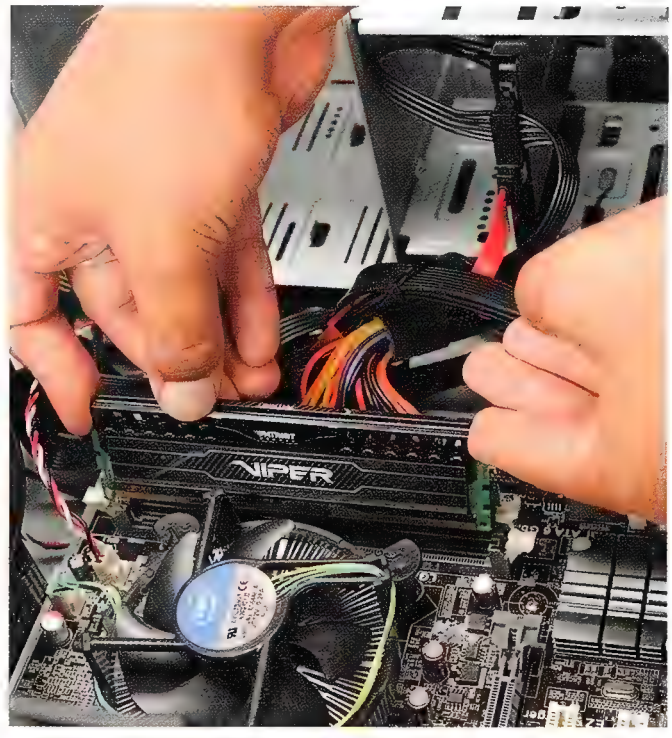
For memory, we'd gone with a low-profile Kingston 4GB kit of DDR3-1333. The kit was about $50 back then and is around $40 now. The Gigabyte GeForce GTX 660 OC got replaced with a more modern GTX 970 in our upgrade. The old GTX 660 cost $300 two years ago, and can be found for $200 online today.

The storage options were modest as well. The A-Data 32GB SSD, 500GB WD Caviar Blue, and Lite-On iHAS DVD+RW didn't exactly set the world on fire, and cost $70, $60 and $22, respectively. The SSD still costs about $70, while the HDD is available for a bit more, at $64. We found the iHAS for $20.

As for the Rosewill case, it's no longer available. When we got it, the basic steel case cost around $70. With a copy of Windows 8 and a PSU, the rig cost $1,200. Without the OS ($120), the total dropped to $1,080. With current pricing and without an OS, the PC would cost about $900 today. That's about the same as a decent GTX 980. As for our upgrades, we gave this little rig new wings at a cost of $1,135.

INGREDIENTS

PART		STREET PRICE
GPU	ASUS GTX970-DCMOC-4GD5	$480
MEMORY	8GB DDR3-1600	$60
PSU	650W 80 PLUS GOLD	$120
HDD	SEAGATE BARRACUDA 1TB	$75
SSD	SAMSUNG 850 EVO 250GB	$150
FAN	CORSAIR AF140 WHITE	$250
TOTAL		$1,135



1 EYE IN THE SKY

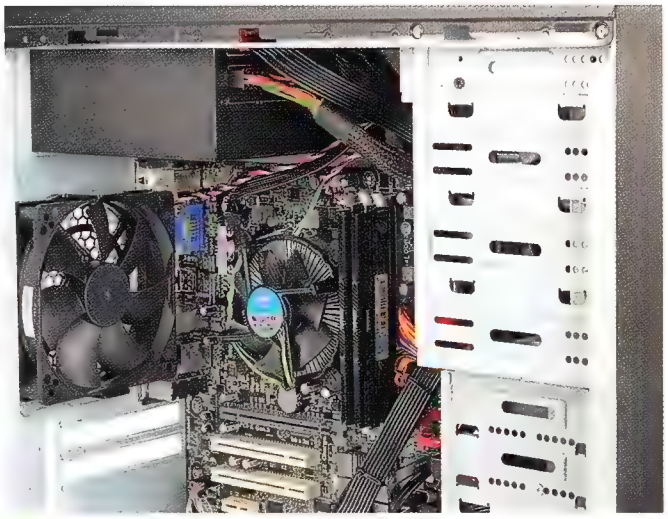
The GTX 970 we upgraded to was by far the most expensive investment in the upgrade. At $480, this GPU is a good $150 more than a GTX 960 that has nearly the same form factor. Since we went with a 660 OC in the original build, we wanted to put in a card that had clear performance gains, but wouldn't let the modest Core i5 hold it back. Even though we regularly build with GTX 980s and above, the GTX 970 is still a very capable graphics card for 1080p gaming.

The GTX 970's modest TDP of 145W meant that we didn't have to go crazy with our power supply, either. The card only takes a single 8-pin power connector, which is nice considering the lack of cable management options in the case.

2 A LITTLE MORE LIFT

We know that it could be argued that 4GB of memory is plenty for a budget rig, but we really feel that 8GB makes the OS and any games feel a lot more comfortable. Browsers, photo editors and audio applications all get memory-hungry now, too. Eight gigabytes should be enough to satiate them in pretty much most circumstances.

These two 4GB 1,600MHz sticks of Patriot's Viper 3 line were taken from a four-stick 16GB kit we had on hand here. While that kit is no longer available, an 8GB kit of DDR3-1600 costs around $60. That's fairly reasonable as RAM prices go, so we didn't hesitate to use these two modules. Another thing to notice is that this mobo only has two DIMM slots, so more RAM would require DIMMs with higher capacity. That costs money, another reason to stick to 8GB.



3 INCREASED LUNG CAPACITY

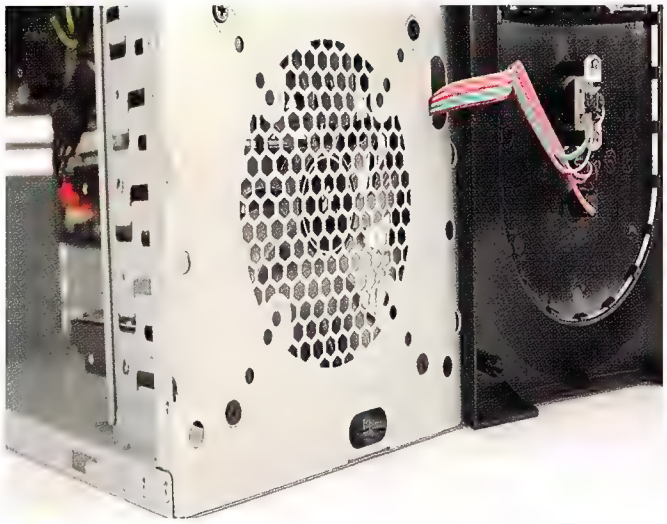
If there's one thing we wanted to upgrade, it was the SSD. Solid-state media has got much cheaper, so we thought it would be reasonable to put money into a higher-capacity and -performance SSD. While the Samsung 850 EVO won't blow your hair back, it's still very speedy. At 250GB, we thought it well worth the $150. For that money, you can have your OS, Steam library and a good number of apps all on one drive.

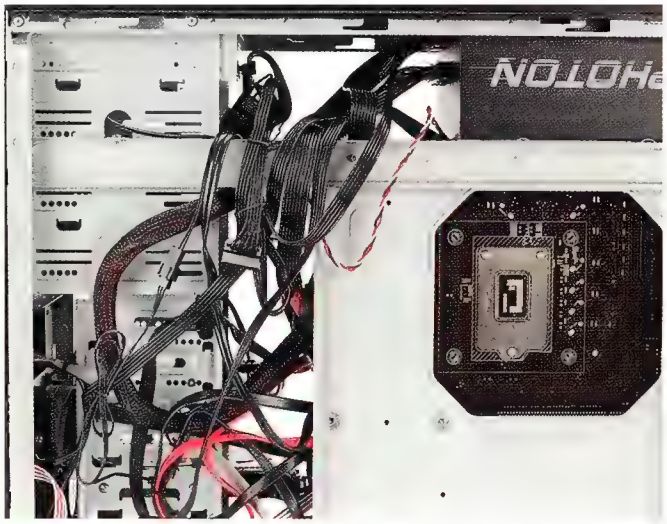
We left in the original 500GB WD Caviar Blue and added in a 1TB Seagate Barracuda. Hard drives can and will fail. Using the Barracuda as a backup for the WD is reasonable. On the flip side, hard drives tend to have a lifespan of about five years. Since this rig is two years old, we could also use the Barracuda as primary storage and the WD as backup for three more years. This should minimise writes and extend the drive's life a little more.

4 INTO THIN AIR

When was the last time you saw a case that mounted the power supply up top? For us, it's been quite a while. With few exceptions, modern cases place PSUs on the bottom. There are plenty of reasons for this: to make way for exhaust fans and cooling radiators, to help dissipate heat more effectively and because installing a heavy PSU above a bunch of pricey components is an unnecessary risk.

We'd used a cheapo 450W PSU with the original build. We decided to replace it with a 650W unit from Corsair. The PSU is 80 Plus Gold certified, which means that it will actually use more of the power it draws from the wall, not just dissipate it as spare heat. The unit also comes with a five-year warranty, which means that by the time you upgrade the CPU and motherboard in this rig, it will probably still have plenty of life left in it.





5 THE JET STREAM

One thing we noticed was the lack of a front fan. With the original configuration, heat wasn't a big issue. And, to be fair, the rear fan has a healthy airflow rate. However, we felt that with an extra HDD and a stock CPU heatsink and fan, a little extra air couldn't hurt.

To install the 140mm Corsair case fan, we had to pry off the plastic front panel. From there, we were able to use case fan screws to attach the white LED fan. Easy enough. What we didn't anticipate was the lack of an extra PWM fan connector on the mobo. The H77H2-M3 only has two PWM pinouts: one for the CPU fan, one for a case fan. Lucky for us, the SATA power cables for this PSU have Molex connectors on their ends. We found a Molex-to-PWM connector and plugged it into one of the SATA cables without a problem.

6 GASP!

Immediately obvious with this case was the utter lack of cable management. In terms of PC cabling, we like our builds to be as organised as possible, but this is the stuff of nightmares. What seems like an obvious route for cables — over the horizontal rail and behind the drive bays — is made impossible by a side panel that has an inward (inward!) bevel. When we tried to keep cabling tucked behind the motherboard tray, we felt like the case was making fun of us. "Oh, that's cute," it would say. "I bet you'd just love an extra centimetre. Tough luck, hotshot."

Coupled with the woefully insufficient zip ties that came with the PSU, this cable job could have you waking up in cold sweats. We had to stuff the cables behind the drive cage, doing our best to keep them out of the way of the front fan's air flow. The wiring still looks like a mess.

1 We didn't bother adding an aftermarket cooler for this Core i5-3350P. The locked CPU doesn't allow for overclocks and is plenty cool, as-is.

2 We didn't go with a Blu-ray and instead stuck with a basic DVD+RW. We popped in a basic Plextor model because, when we found this box, the original drive was missing.

3 Only two of the six SATA cables have horizontal ports, which excluded longer GPUs from being used on this mobo. Luckily, our GTX 970 is pretty short.

4 The long grey ribbon cable is for the front panel audio. We had to make sure we disconnected this before removing the panel to prevent bent pins.

EXHALE

When we set out on this project, we specifically wanted to revisit an older build. Sometimes, upgrading an old PC can feel like hooking up with an old friend you've lost contact with. Some things carry over from the past, but new additions make it different.

However, this wasn't a single cheap upgrade. The total cost of parts we used in the upgrade almost exceeded the original cost of the PC. That said, upgrading the CPU and motherboard would have added another several hundred pounds. By holding on to a slightly older motherboard and CPU, we still got a respectable PC for less than the price of a new one. That's not bad, if budget is an issue.

And speaking of budget, these upgrades are totally do-able as incremental upgrades over time. Adding a fan, storage and RAM is relatively cheap and easy to do. The graphics is more expensive to modernise, especially since the PSU upgrade is a good idea for the new GPU. But as time goes by, upgrading the case, motherboard and CPU are certainly possible upgrades that could make this PC more current.

This rig really chugged along in our timed benchmarks. It took half an hour for it to finish the ProShow export, and almost 20 minutes to finish stitching photos. Even though it had four cores, the modest CPU crunched numbers at a pokey 10.3 frames per second in our x264 benchmark. In our graphics benchmarks, the GTX 970 made a respectable showing. In 3DMark FireStrike Ultra, this build beat another budget build we have, costing about $1,250, which sports a GTX 960 and i5-4590. It scored about 700 points lower than a $2,300 mainstream build of ours with a i7-4790K and GTX 980.

> "However, this wasn't a single cheap upgrade. The total cost of parts we used in the upgrade almost exceeded the original cost of the PC."

That midrange PC's CPU and GPU combo alone costs $1,400 — more than all the combined upgrades that went into this build, not to mention that its CPU is also sitting on a more expensive Z97 board ($280). All things considered, these upgrades provide a marked improvement in performance at a reasonable price.

As for the game benchmarks, *Batman: Arkham City* showed an enjoyably playable 70fps at 1440p, which lets us know that other games will fare well at 1080p.

LABS RESULTS: UPGRADED SYSTEM BENCHMARKS

	THIS PC	APC LABS GRAPHICS TEST RIG (% CHANGE)
STITCH.EFX 2.0 (SEC)	806	1,165 (-44.5%)
PROSHOW PRODUCER 5.0 (SEC)	1,472	1,805 (-22.6%)
X264 HD 5.0 (FPS)	33.8	10.3 (-69.5%)
BATMAN: ARKHAM CITY 1440P (FPS)	204	70 (-65.7%)
TOMB RAIDER 2160P (FPS)	87.5	28.6 (-67.3%)
SHADOW OF MORDOR 2160P (FPS)	70.1	30.6 (-56.3%)
3DMARK FIRESTRIKE ULTRA	8,016	2,484 (-69.0%)

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Our test rig PC uses a Core i7-5960X CPU, three GTX 980s and 16GB of RAM. *Arkham City* tested at 2,560 x 1,440 max settings with PhysX off; *Tomb Raider* tested at ultimate settings; *Shadow of Mordor* at max settings.

Create a Pi-powered media PC

Mayank Sharma explains how you can upgrade to the latest OpenELEC 14 and take your home-entertainment setup to the next level.

You can use the Raspberry Pi to do all kinds of geeky things, but one of the most interesting uses for the little device is that of a home theatre PC (or HTPC). The small size of the hardware and the fact that it runs silently make it a really good choice for building your own entertainment centre.

One of the best open source apps for turning any computer into a fully functional media centre PC is the recently rechristened Kodi media player, formerly known as XBMC. Kodi uses a 10-foot user interface, which is ideal for connecting to large-screen displays and projectors and thanks to ergonomic display elements it can be easily navigated using a remote control. You can also control playback using your Android smartphone.

Using Kodi you can view multimedia in virtually any format. Besides playing files from local and network storage devices, Kodi can also fetch files from online services, such as YouTube, Spotify, Pandora Radio and more. While you can install Kodi on top of Raspbian, there are several projects that produce a dedicated media centre distro for the ARM-based device, including OpenELEC. The OpenELEC project produces streamlined builds based on Kodi for various platforms, including the Raspberry Pi.

The advantage with OpenELEC is that you can use the distro without any knowledge of its base Linux OS.

DOWNLOAD OPENELEC

To start setting up your HTPC, grab the OpenELEC build for the Raspberry Pi. As with other projects, OpenELEC hosts different images for the older single-core Raspberry Pis and the newer quad-core ones. Once you've downloaded the image, extract it and transfer it on to an SD card, either from Linux using the dd command, as follows

```
sudo dd if=OpenELEC-RPi2.
arm-5.0.8.img of=/dev/sdd
```

or from Windows using Win32 Disk Imager.

Then you need to insert the card into the Raspberry Pi, hook it up to your TV via the HDMI port and power it on. OpenELEC boots up pretty quickly and will take you straight into Kodi. If you've used the media player (or its predecessor XMBC) before on the desktop, you shouldn't have any issues navigating it on the Pi. However, you will need to spend some time configuring the media centre to take advantage of this specialised environment.

Use your keyboard to scroll through

Optimise playback

Although the Raspberry Pi 2 packs quite a punch, there are some tweaks you can do in OpenELEC that result in smoother playback. For starters, you can turn down the video playback resolution to 720p, especially if your HTPC isn't connected to a Full HDTV. Head to Settings > System > Video Output, and change the Resolution option to 720p.

Another trick is to replace the default skin, which was designed for desktop computers, to a lightweight skin, such as Aeon Nox, which makes navigating the menus snappier. To change the skin, head to Settings > Skins. Also make sure that hardware acceleration is turned on. Go to System > Video > Acceleration and check that the Decoding Method is set to 'Hardware' and not 'Software'. While you're here, also reduce the GUI updates when playing video to 5fps.

Another playback-related tweak involves matching the refresh rate of the screen to the video being watched, which results in smoother playback. You can enable it by going to Settings > System > Video > Playback, then toggle the 'Adjust Display Refresh Rate' to 'Match Video'.

Another way to smooth out playback is to use audio passthrough for encoded audio, such as Dolby. To enable the option, navigate to Settings > System > Audio Output and toggle the 'Enable Passthrough' option. Finally, if you are on a slow internet connection, you can cut down on the bandwidth usage by heading to Settings > Video > Library and disabling the 'Download Actor Thumbnails' option.

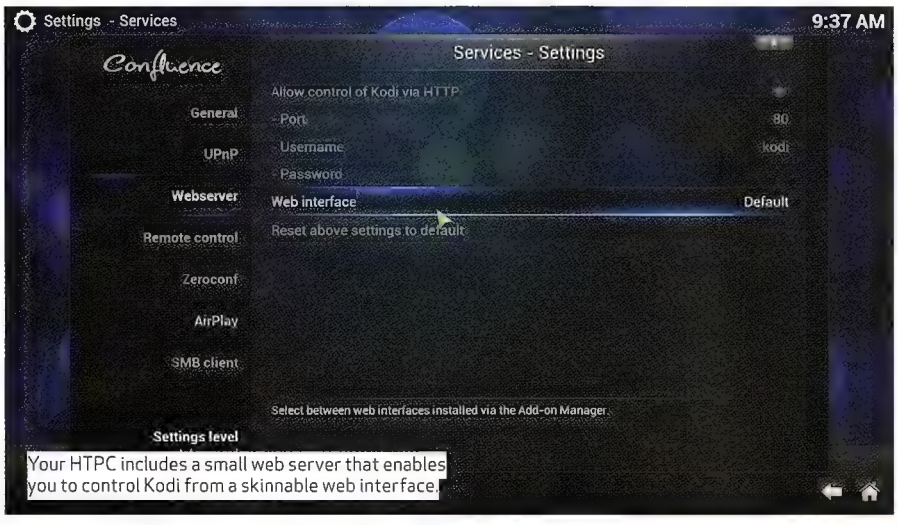
Back up your video library

Seeing as you've spent a considerable amount of time setting up your HTPC, it would be a shame to lose it all because of a corrupted card. To prevent this happening, you can back up all your customisations and information about your library. Kodi includes a backup utility, but we'll use an add-on that enables us to back up files to a custom location, including Dropbox.

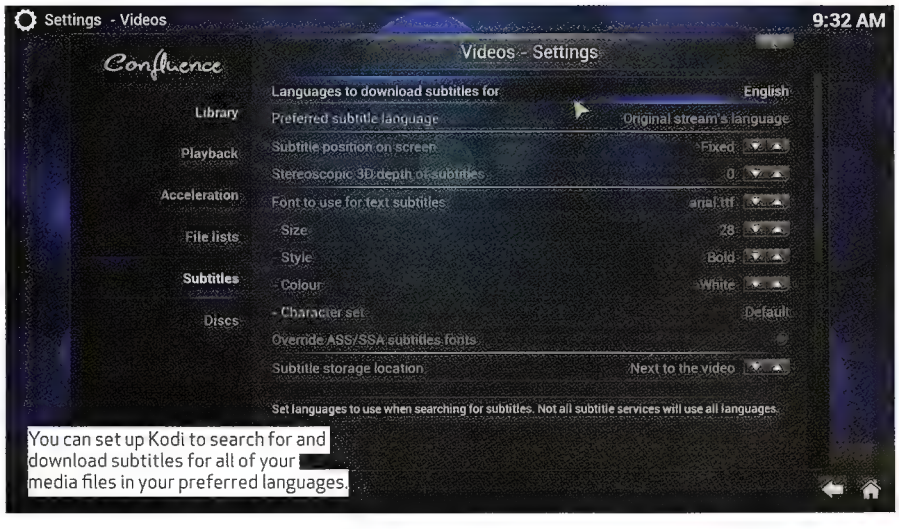
Head to Programs > Get More and install the Backup add-on. Once installed, launch it from under Program > Backup. The program asks you to select one of two modes – 'Backup' or 'Restore'. When you select 'Backup', it throws an error because we haven't configured it yet. Simply click 'OK' to bring up the Settings window.

If you wish to back up to Dropbox, use the Remote Path Type pull-down menu to select the 'Dropbox' option, and enter the authentication details for your Dropbox account. Otherwise, click 'Browse Remote Path' and select the location where you wish to store the backup files. Optionally, select the 'Compress Archive' option to reduce the size of the backed-up files. Then switch over to the File Selection tab and customise the list of files you want to back up. Finally, switch over to the Scheduling tab and enable the scheduler to back up automatically, as per your defined schedule.

Once you've set it up, create an initial backup copy by launching the Backup program. This time when you hit the 'Backup' button, the program saves the marked files to the specified destination. To restore the files, simply launch the program and click the 'Restore' button. The program shows you a list of all the backups inside the configured backup location.



Your HTPC includes a small web server that enables you to control Kodi from a skinnable web interface.



You can set up Kodi to search for and download subtitles for all of your media files in your preferred languages.

the Kodi menu and head to System > OpenELEC. This section lists settings and configuration options related to the distro under five different categories. From the System category, you can change the hostname of this OpenELEC installation. This is handy for distinguishing multiple instances, in case you have more than one system on your network – one in the living room, say, and another in the bedroom or kitchen.

Also, by default, OpenELEC is set up to inform you when a new update is available. However, you can toggle the Automatic Updates option and ask the distro to fetch the update without asking for your approval.

For a better HTPC experience, you can use OpenELEC with a Raspberry Pi-compatible Wi-Fi adaptor. Once you've connected the adaptor, head to System > OpenELEC > Network, and toggle the Active option under the Wireless Networks section. Then switch to the Connections section and select your Wi-Fi network from the list that appears there. Now you'll need to click 'Connect' and enter the relevant authentication details to connect to your home Wi-Fi network.

There are also a whole host of settings available in Kodi , which are listed under Settings > System. Using these settings you can configure such things as audio output, calibrate the monitor, set up remote controls and set up Kodi's built-in PVR.

To watch TV on your Raspberry Pi HTPC, head to Settings > System > Live TV, and toggle the Enabled option. You will then be asked to enable one of the supported PVR add-ons. Select your PVR from the list and click the 'Configure' button to enter the relevant configuration details, such as the IP address of the PVR host. When you're done, click the Enable button to activate it. Then head back to the System > Live TV section to set up other options, such as altering the behaviour of the onscreen display, the length of the recording and parental controls etc.

ADD AND STREAM CONTENT

Once you've set it up, it's time to add content to your HTPC. You can configure a bunch of media sources in Kodi: these media sources can be local media on the card, removable USB drives plugged into the Pi and even file shares on the local network.

To define a media source, enter any of the Videos, Music or Pictures entries on the screen, and click Add Sources. Use the dialog box that pops up to browse to a source that contains some media. Adding media on the card or plugged-in USB drives is pretty simple and straightforward. But if you wish to pull in content from another computer on the local network, you have to define the network shares first.

Kodi supports several file-sharing

protocols, including Samba, NFS, AFP, FTP and more. To view media on a shared Samba drive, head to System > OpenELEC > Services, and toggle the Enable Samba option. If the source requires authentication, toggle the Use Samba Password Authentication option and enter the username and password. When you've added a source, you can tell Kodi about the type of content it houses. In return, Kodi allows you to choose a scraper – a special plugin that fetches metadata about a media file from the internet. If you've set up multiple OpenELEC HTPCs on the same network, they can also share libraries between them, using the UPnP protocol.

On the HTPC that houses the content you wish to share with the other HTPC, head to Settings > Services > UPnP and toggle the 'Share Video and Music Libraries Through UPnP' option. Now jump over to the other HTPC where you wish to view the content, and add a source (as described earlier). When you browse for a media source, select the 'UPnP Devices' option from the list of sources, which then displays the other HTPC that houses the content.

REMOTE PLAYBACK CONTROL

Your HTPC will now enable you to watch content either on locally connected drives or on any other computer or HTPC on the network, and even from your DVR. To further enhance the experience, you can enable the web interface to remotely control playback. Kodi includes a web server which allows you to control the player via a web browser. To enable it, head to Settings > Services > Webserver and toggle the 'Allow Control of Kodi Via HTTP' option. You can lock access behind a password, if desired. Once enabled, fire up a web browser on any PC on the network and navigate to the IP address of the HTPC to control playback.

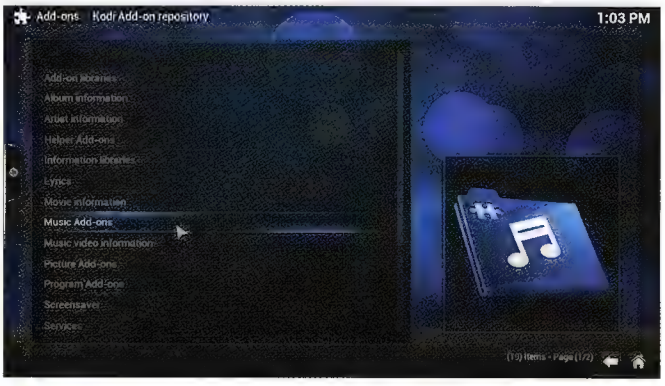
Kodi also produces official remote control apps for Android and iOS devices, and, shockingly enough, you can find several third-party ones for the Windows Phone as well. Before you can use them, head to Settings > Services > Remote Control, and toggle the 'Allow Program on Other Systems to Control Kodi' option. Now head to your device's app store and grab a remote control app. The official app is called Kore on the Google Play Store.

Extend with add-ons

Add-ons - Get Add-ons
3:35 PM
SuperRepo All (helix)
SuperRepo.org
Author: Bart Otten
Version: 0.5.208
Download and install add-ons in the category "All" from the SuperRepo.org addon repository.
If you find a broken or not working addon or you would like to include another one, please have a look at https://superrepo.org/
The repository is maintained by the Kodi community using the SuperRepo Wiki and our generator fetches

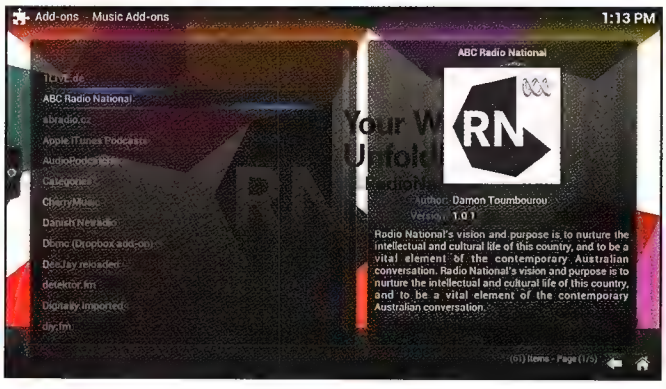
1 SELECT A REPOSITORY

You can extend virtually every aspect of your HTPC by adding a number of plugins and extensions. To do this, head to System > Settings > Add-ons > Get Add-ons. This displays a list of repositories (repos), including the official OpenELEC and Kodi repo. Select the repo you wish to install from. There's also the All Add-ons option, which displays plugins from both these repos.



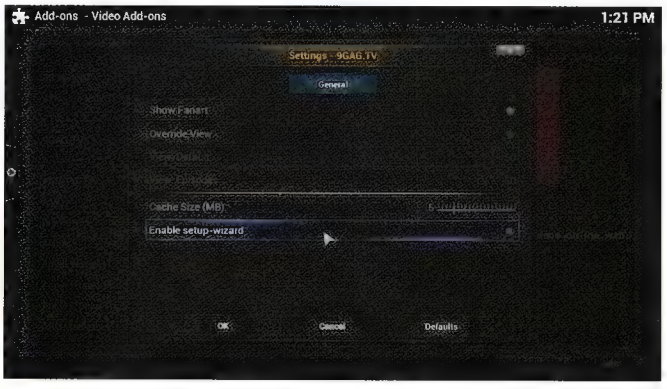
2 SELECT CATEGORY

Once you've selected a repo, you're shown a list of add-on categories. The Kodi repo includes a lot more categories than the OpenELEC one. The OpenELEC repo mostly includes drivers for various devices, while the Kodi repo includes well over a dozen categories. The Programs Add-ons category is particularly interesting and houses plugins that turn your HTPC into a seed box.


Add-ons - Music Add-ons
1:13 PM
ABC Radio National
Author: Damon Toumbourou
Version: 1.0.1
Radio National's vision and purpose is to nurture the intellectual and cultural life of this country, and to be a vital element of the contemporary Australian conversation. Radio National's vision and purpose is to nurture the intellectual and cultural life of this country, and to be a vital element of the contemporary Australian conversation.

3 SELECT THE ADD-ON

When you select a category, you're shown a list of related add-ons. For example, if you select the Music Add-ons category, you're shown plugins for various online radio stations. Similarly, the Video Add-ons category houses plugins for popular video streaming websites, including YouTube, Vimeo and TED Talks. When you find a plugin you wish to use, select it and click the 'Install' button.



4 CONFIGURE THE ADD-ON

You're returned to the list of plugins while Kodi downloads the one you selected. Kodi also installs and enables the plugin with the default options. Some plugins have optional configurable elements. To view these, click the 'Configure' button associated with the plugin. The installed plugin is accessible from under its category, eg video plugins install under Video on the main page.

Must-have add-ons

Add-ons - Picture Add-ons
5:40 PM
Add-on information
PicasaWeb
Type: Media sources
Author: Rick Phillips (nuuk)
Version: 1.0.2
Summary: ...in to browse PicasaWeb albums and photos/videos
Description
Page (1/1)
Browse your PicasaWeb albums and tags. Browse your favorite user's albums, tags, and their favorite users. Search your photos/videos, your contact's photos/videos, and search PicasaWeb. View maps of photos with geo location data.
Install
Change log
...lib-python

Videos - TED Talks
5:47 PM
Alice Goffman: How we're primed some kids for colleg... 05/01/2015
Sophie Scott: Why we laugh 04/30/2015
Greg Gage: How to control someone else's arm with yo... 04/28/2015
Nick Bostrom: What happens when our computers get... 04/27/2015
Nizar Ibrahim: How we unearthed the spinosaurus 04/24/2015
Clint Smith: How to raise a black son in America 04/23/2015
Chris Milk: How virtual reality can create the ultimate e... 04/22/2015
Jeddah Isler: How I fell in love with quasars, blazars a... 04/21/2015
Gary Haugen: The hidden reason for poverty the world... 04/20/2015
...he secret to the origin of life | Nathalie Gabriel: How it... 04/17/2015
Paul Tudor Jones II: Why we need to rethink capitalism 04/16/2015
Takaharu Tezuka: The best kindergarten you've ever seen 04/14/2015
Kailash Satyarthi: How to make peace? Get angry 04/03/2015

1 BROWSE IMAGES

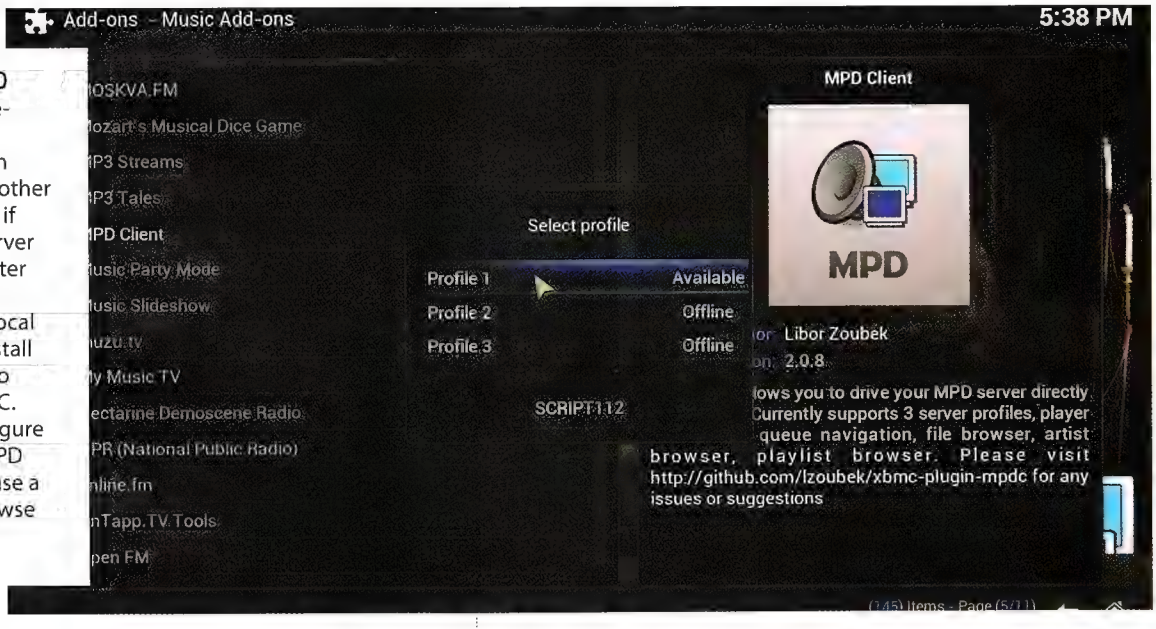
You can find lots of inspiring pictures on websites such as Flickr and PicasaWeb. Head to the Pictures Add-ons section, which lists plugins that enable you to pull in images from these websites, and others such as the Hubble Space Telescope. Once enabled, different websites give you different options, eg Flickr includes a list of interesting Images of the Day and runs a slideshow of them.

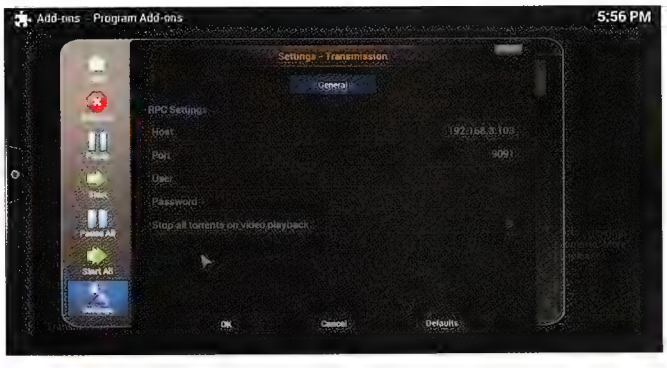
2 WATCH ONLINE VIDEO

Similarly, there are lots of video streaming websites, such as YouTube, Vimeo, NASA TV, TED Talks etc. You can find add-ons for each of them and others inside the Video Add-ons section. Each add-on lists videos according to the service it supports. For example, TED Talks lets you browse by topics or speakers, while NASA TV and YouTube have both live and recorded videostreams.

3 CONTROL MPD

Besides remote-controlling content on the HTPC, you can control playback on other machines as well. So if you have an MPD server running on a computer (or a Raspberry Pi) somewhere on the local network, you can install the MPD Client Audio add-on on your HTPC. Once installed, configure it to point to your MPD server and you can use a nice interface to browse through music and control playback.





4 MONITOR DOWNLOADS

There are other things you can control remotely, eg you can connect to, monitor and control downloads on a remote computer. The Transmission Client add-on available under Programs can connect to another Transmission client on the network. For this to work, you need to enable the Remote Control feature in the Transmission client on the desktop, under the Edit > Preferences > Remote tab.

5 PLAY CLASSIC GAMES

Another attractive add-on under the Program is the ROM Collection Browser. Once enabled, the add-on takes you through a wizard to set itself up according to your environment. It then imports your ROMs, scrapes metadata about them from online sources and allows you to play your classic games. Setting it up is quite involved, so go to **http://bit.ly/ROMCollectionBrowser** to get it to work.

Turn your Android into a video monitor

We've seen how Android devices can capture CD-quality stereo audio. But a smartphone video monitor? Darren Yates shows how it's done.

Android has come a long way since the original Android 1.0 release. But so, too, has the hardware. Four years ago, your typical Android smartphone this side of $200 outright plodded along with a 528MHz single-core ARM11-grade CPU, a sprinkling of RAM and an Android version still starting in the '2's. Today, you can pick up a quad-core Cortex A7 tablet with USB2.0 OTG port for under the $100 mark. That extra CPU horsepower has made a huge difference to everything from gaming and HD video to audio capture, as we saw last month. But that amount of speed also now makes it possible to turn your smartphone into a video monitor.

TOTAL RUBBISH

Some readers are no doubt ready to gently point out, "Mate, see that little black dot on the back of your phone? It's called a 'camera', you boofhead!" And yes, it is – but that's not the only source of live video you can view on your smartphone, not by a long shot. Thanks to the combination of various factors from improved driver support to low-cost hardware, plus some interesting apps from Google Play, we've found four different devices and tested three of them that give you plenty of live video feed options beyond the 'little black dot'.

COMPOSITE VIDEO INPUT

You've no doubt seen those compact little USB video grabber devices – the USB thumb drive-style device with cables poking out the other end?

The EasyCap video dongle output can be viewed on your Android phone.

They've been popular on PCs for years and even more so on eBay – you'll find them selling for as little as $7. They allow you to capture analog composite or S-video input and stereo analog sound into your PC, usually for making home DVD movies. However, it turns out that with the right combination of device and software, you can connect and view that same video feed right on your Android phone or tablet.

Online, these devices typically sell under the 'EasyCap' brand, but the trick for us is combining them with the EasyCap Viewer app on Google Play (**tinyurl.com/o9qel7c**) – it'll cost you about $6 and while the app isn't exactly rock-solid stable, for the right application, it's well worth the price. The software supports only two EasyCap versions – yes, there's more than one, unfortunately – one with an STK1160 chip, the other with a UTV007 chip, and we're told you want the one with the UTV007 chip.

But just to make things more difficult, the only way to tell which chip you get is for the seller to tell you. But as we found out, it's more accurate to just buy one and pull it apart.

So that's what we did – we purchased one in Australia for under $10, it arrived, we prized the top off, looked at the chip and found – HTV600. We tried it on a couple of USB camera apps on our Lollipop'd Galaxy S3 phone and the closest we got to anything working was one app recognizing that, yes, we'd connected up a USB device. We had the same result on our original Android 4.0.3-powered Acer Aspire A200 tablet.

MIX AND MATCH

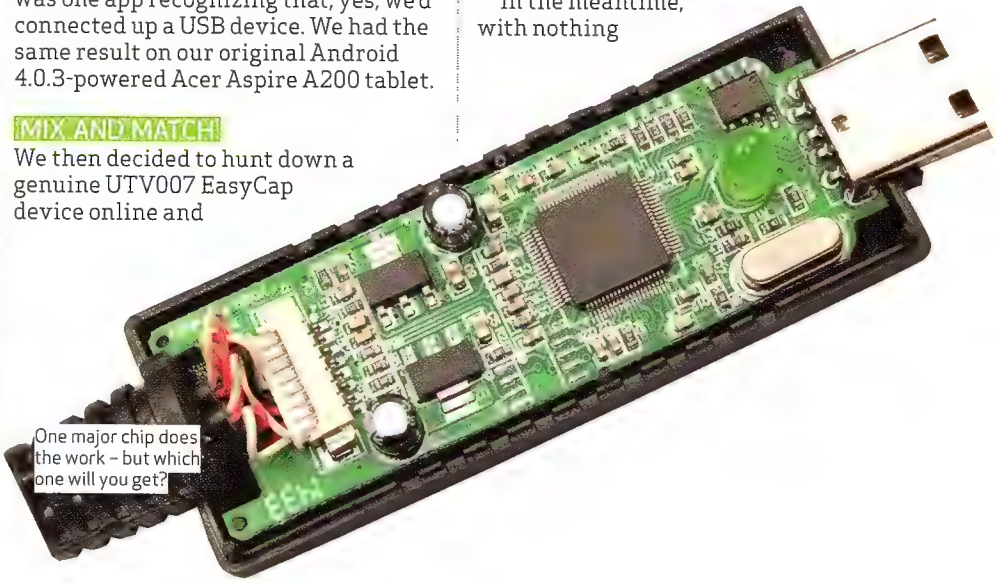
We then decided to hunt down a genuine UTV007 EasyCap device online and found an eBay supplier noted for selling ridgy-didge UTV007 EasyCaps for $12. So, we bought one, it arrived, we prized the top off, looked at the chip and found – HTV600. Thinking we'd stumbled onto 'Groundhog Day', I got back to the eBay supplier quick-sticks, asking for a 'please explain'.

'Oh, no, we sell UTV007'.

I shot back with a photo to prove that this wasn't the case.

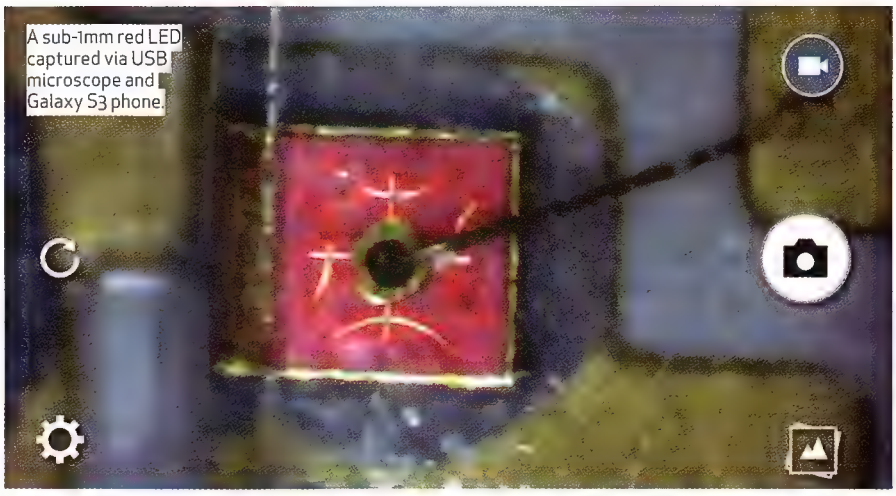
In the meantime, with nothing

Six LEDs light up this $13 inspection camera via the USB plug's thumb scroll.

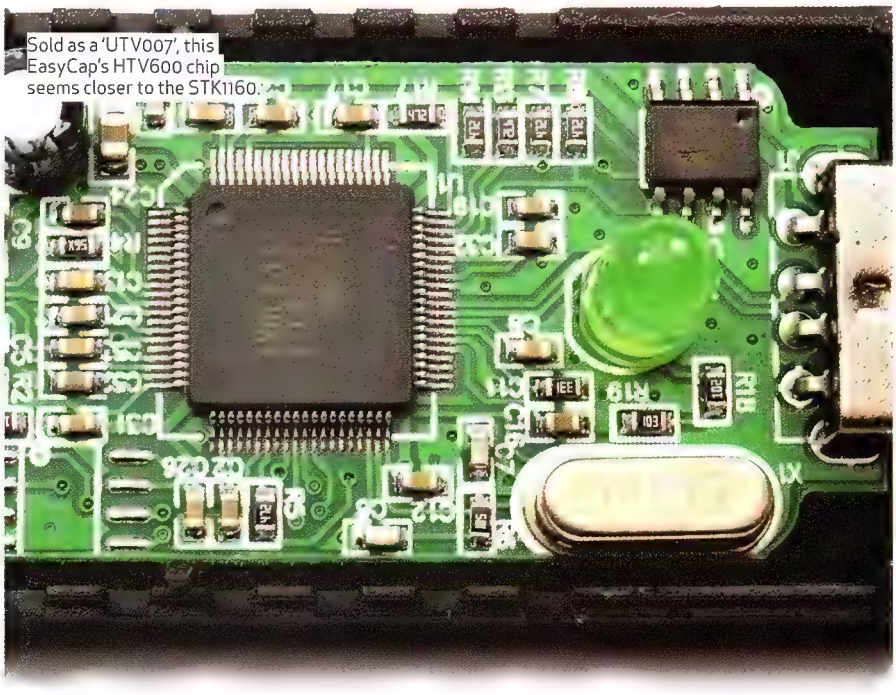


One major chip does the work – but which one will you get?

A tiny, narrow 30fps VGA camera with five metres of cable for $13.



A sub-1mm red LED captured via USB microscope and Galaxy S3 phone.



Sold as a 'UTV007', this EasyCap's HTV600 chip seems closer to the STK1160.

left for it, I took one of my now-two HTV600-chipped EasyCaps, plugged it into the USB-OTG cable and into the phone, purchased the EasyCap Viewer app and pottered off in search of some composite video input. Plug it into an old VHS recorder, turn it on, fire up the Viewer app and knock me over if I didn't see the video feed on the phone panel! It looked decidedly like an analog feed being digitised, but nevertheless, it was relatively clean, no jitter and full 25fps frame rate. The app itself supports NTSC and PAL-standard video and provided your composite video source fits either of those, it can really come from just about anywhere.

The next day, the eBay seller got back to me, a little sheepish, saying 'it is same chip, just new number'. Given what I found the previous day, there was little point arguing. In the end, the device worked — just not quite the way I expected.

SO WHAT?

The EasyCap Viewer app is relatively new and supposedly only supports those STK1160 and UTV007 chips. I didn't have to change anything (default was set to STK1160) and it worked on the HTV600 devices. However, the thing is if you plug in the device, launch the app without a video feed into the EasyCap dongle, the app crashes saying 'I/O error'. But as we found out, there's a trick to the way it works — you have to provide a video feed into the EasyCap before you start the app. Then, it's as happy as pie and away it goes. The downside with the app for now is that there's no audio or video recording, but according to the app developer, that's on the way.

With no sound or video recording, you're probably thinking why on earth would you bother? Sure, it's not for everyone, but if you're into FPV miniquad racing, this is about the cheapest way of creating a portable video monitor for the FPV (first-person view) video signal from your (sorry to use the word) drone's camera receiver. Video goggles are the ideal way to enjoy your white-knuckle ride, but with most google kits starting at around $400, your phone or tablet as an FPV monitor for $10 is a much cheaper way to start out.

According to the EasyCap Viewer developer, you only need ICS/Android 4.0 or newer, so if you have an old Tegra 2-powered 10-inch tablet (like the Acer Aspire A200), it could be the perfect way to get a battery-powered FPV monitor happening on the cheap.

The usual caveats apply and your mileage may vary, but it's definitely worth a look.

ENDOSCOPE/BORESCOPE INSPECTION CAMERA

They go under various names from 'endoscope' or 'borescope' to generic 'inspection cameras', but they're basically a video camera on the end of a length of cable that plugs into a specialised hand-held video monitor. As their names suggest, they're used for disappearing up things; cable pipes, drains and... well, you get the idea.

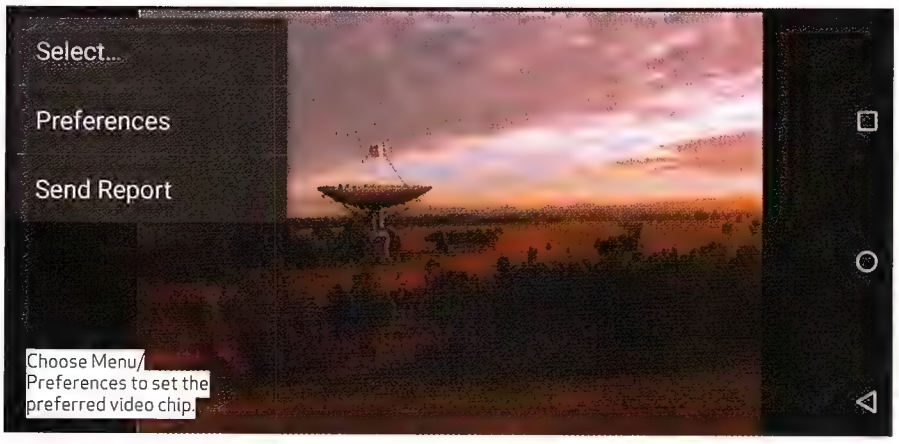
But they're also now becoming silly-cheap on eBay. We picked up a five-metre inspection camera for just $15. On one end, you get a tiny camera unit that's not much larger in diameter than the actual cable and has six tiny white LEDs embedded on the front. On the other, a standard Type-A USB plug. We plugged it into a USB-OTG cable, whacked the other end into the Galaxy S3, tried out our cache of USB camera apps and up came the video image on the phone panel.

USB CAMERA APPS

When it comes to USB camera devices, you need to have three free apps from Google Play installed on your Android device — simply because there appears to be no rhyme or reason as to which

Subpixels of a Samsung Galaxy S2 via USB microscope taken on a Galaxy S3.

HTV600 owners should set EasyCap Viewer to STK1160 option.



Choose Menu/ Preferences to set the preferred video chip.

The EasyCap dongle can give your phone/tablet a composite video input.

one of those apps is going to work. So, head to Google Play and install CameraFi, Dashcam and UsbWebCamera. As we said, they're all free – you just have to make sure you're using an Android device with at least ICS/Android 4.0 and a USB-OTG or USB host port ready to go.

Each of these apps appears to come with its own USB Video Class (UVC) drivers and for the most part, you'll find budget camera devices today support this 'driver-free' standard. But the mysteries of combining Android device, Android OS, camera device and app are such that you can never predict which combo is going to work, but you should find something that does.

We have to admit the $15 borescope's video image quality wasn't brilliant (smoky lens cover and LED flare didn't help), but short of sticking your head in a pipe or wall cavity, it worked enough for the price.

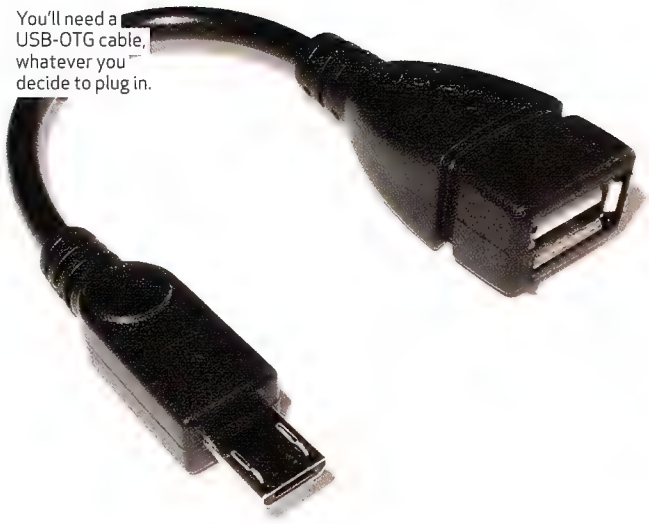
USB MICROSCOPE

Over the last year or so, we've seen a number of almost-zero-cost hacks turning the built-in camera from a smartphone into a more-than-passable microscope. One option is to tape or print a 3D attachment that clamps a tiny borosilicate glass bead to the camera lens. Another, invented by Dr. Steve Lee from the Australian National University's Research School of Engineering, is to create droplets of a silicon polymer called 'polydimethylsiloxane' or PDMS. Gravity creates the droplets, an oven bakes them until hardened, turning them into super-cheap magnifying lenses with as much as 160X magnification power (**tinyurl.com/pyc8xu5**).

However, there is another alternative that doesn't use beads or polymer-baking – and that's a USB microscope. We looked at these a few months ago, but we've been that impressed with how ours works on Android, we thought it definitely worth another run. They're basically a VGA camera behind a plastic zoom lens with a clamp holder and base. For all intents and purposes, they're the same class of device as the inspection camera above and we've found them now online for as little as $16.

Again, you plug it into a USB-OTG port and into your Android device, launch one of the three USB camera apps we've already mentioned and eventually with the right combo, you get a video image on your device panel. Zoom in, grab a screenshot of your image and you're done.

Granted, a USB scope is more expensive than borosilicate glass beads or PDMS polymer droplets, nor can we guarantee it'll work on all Android devices. But it's nowhere near



You'll need a USB-OTG cable, whatever you decide to plug in.

Hotspot on a phone: Seek Thermal's thermal imaging module for Android.

as messy and has the benefit of variable zoom.

We bought our USB microscope a couple of years ago for around $35, so the fact they're now down to $16 suggests (the falling Aussie dollar notwithstanding) they're about as cheap as they to get. For school science labs, for example, it could be worth buying one and trying it out, but you probably don't need an excuse.

All of the basic models we've seen come with a ring of nine white LEDs inside the clear front shroud and an in-line rotary brightness control near the Type-A plug end of the cable. You won't discover a cure for cancer with one of these, but for delving down and looking at close detail of anything from surface-mount LEDs to phone panels, for example, it's not a bad option. Again, your mileage may vary.

THERMAL IMAGING CAMERA

These aren't sold in Australia yet, but as soon as they are, we'd love to get one into Labs for a look-see. Seek Thermal (thermal.com/thermal-cameras) makes tiny thermal imaging camera phone modules that plug into Samsung Galaxy S3/S4/S5 smartphones and Note 2/3/4/Edge phablets. There's also a Lightning-version for iOS devices.

They're a 206x156-pixel thermal imaging sensor powered by and plugging straight into the microUSB/OTG port on the bottom of your phone/tablet. Temp reading speed is generally less than 9Hz, but detection range is from -40-degreesC to 330-degreesC over a 36-degree field-of-view. Think of it has having 32,000 infrared temperature sensors all working at the same time.

The Seek Thermal module might well be near enough to $400, but given the starting price for a basic FLIR handheld imaging camera in Australia is around $1,000, it's arguably the cheapest device available. That said, if you're ready for some home-DIY, US company Melexis makes a 16x4-array thermal image sensor called the MLX90621 (**tinyurl.com/odpjnmo**) for around US$70 that apparently can be used with an Arduino board, but that's another story.

WHO NEEDS A PC?

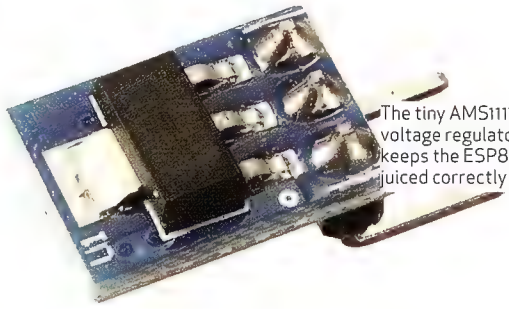
What's exciting about Android is that now we've got over the 'first flushes of youth', the platform is maturing with USB driver and connectivity improvements. Android devices are the embodiment of the 'personal computer' and as processing power and performance start to give traditional PCs a nudge, so come the traditional PC applications such as audio and video capture. And with the arrival of USB Type-C, it'll be interesting to see just what new devices appear to turn smartphones into all sorts of gadgets.

In the meantime, we know there's much more video to be had than what you get from that 'little black dot'. ■

This USB microscope's LEDs are controlled by inline cable scroll wheel.

USB VGA microscopes now sell for under $20 online.

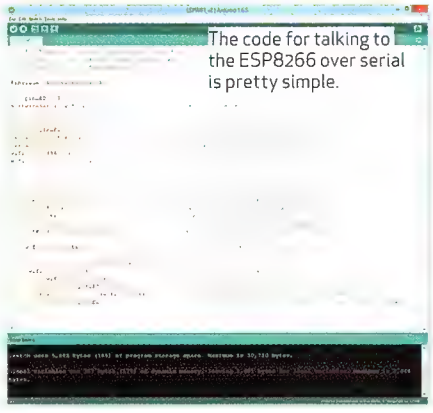
Arduino Wi-Fi – Part 1



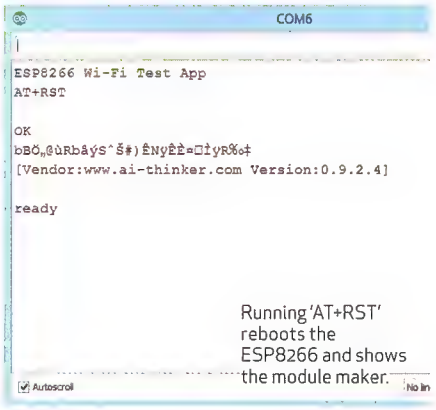
The tiny AMS1117-3.3 voltage regulators keeps the ESP8266 juiced correctly

Connecting your projects to the web doesn't need expensive tech. Darren Yates shows how to add 802.11b/g/n Wi-Fi for less than $5.

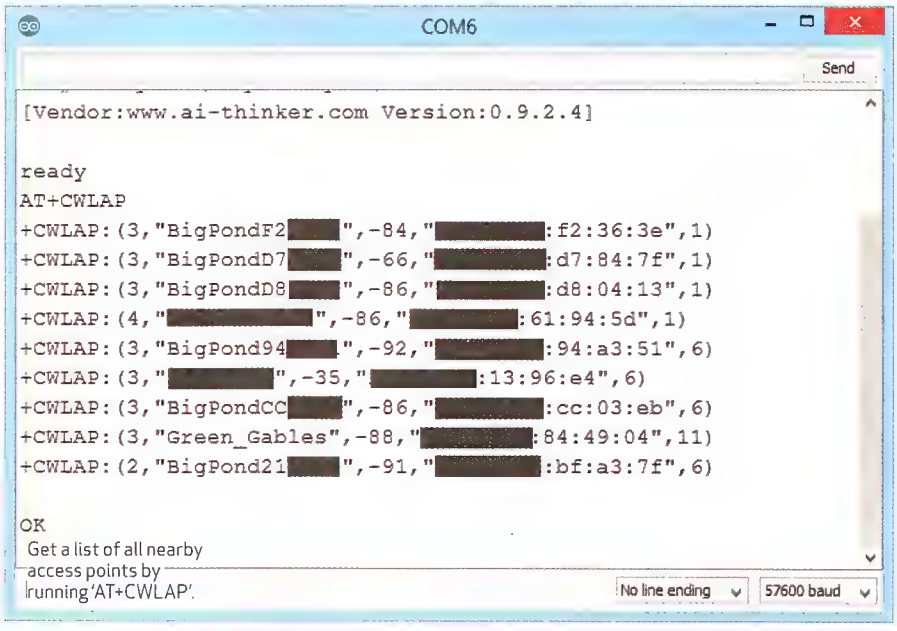
Two things make the current Internet of Things (IoT) craze possible – one is the crazy-cheap microcontroller chips flooding the market, like the Atmel ATMEGA328P found in our Arduino Uno board. The other is the new range of powerful, low-cost Wi-Fi controller chips appearing everywhere. These chips, that also include their own microcontroller inside, are cutting the cost of incorporating Wi-Fi into new gadgets by a factor of ten, providing enormous savings. And the chip doing most of the price damage is Espressif Systems' ESP8266 (tinyurl.com/qa3d7ed).



The code for talking to the ESP8266 over serial is pretty simple.



Running 'AT+RST' reboots the ESP8266 and shows the module maker.



Get a list of all nearby access points by running 'AT+CWLAP'.

WI-FI ON A CHIP

The ESP8266 contains a full Wi-Fi transceiver with built-in RF power amplifier. It'll work as a software-based access point (use it as a client or a server), it supports 802.11b/g/n standards and it even has a 32-bit microcontroller CPU on-board you can program to do other things.

However, the simplest way to use it is part of a low-cost module, the most common being the 'ESP-01'. This tiny 8-pin module is smaller than an SD card and can be made to work with almost any microcontroller, including the Arduino series. You'll find it on eBay for under $5 including shipping.

HOW IT WORKS

The ESP8266 works like an old analog modem – that's because you drive it as a serial device from your Arduino using Hayes AT-style commands. The most complicated thing about it is it's designed to work on a 3.3VDC voltage supply whereas most Arduino boards run off 5VDC. Feed 5VDC straight into the ESP8266 and it's pretty much toast. The solution is to use a voltage regulator chip. We're using a three-pin module based on the AMS1117-3.3 regulator. It's smaller than a microSD card, sells for around $1 on eBay and works perfectly, regulating the incoming voltage to a rock-steady 3.3VDC output.

The ESP8266 only has two data pins that matter – TX (transmit) and RX (receive). Now the ESP8255 being '5V-intolerant' suggests putting 5VDC on its pins blows it up. However, we've been using the layout shown for several weeks without an issue. The key is ensuring the voltage rail to the module is 3.3VDC.

SIMPLE APP

We'll get cracking with a simple Serial I/O app that allows you to communicate with the ESP8266 chip over the Arduino IDE (Integrated Development Environment) Serial Monitor. The Serial Monitor is Arduino's way of allowing you to code feedback from your projects.

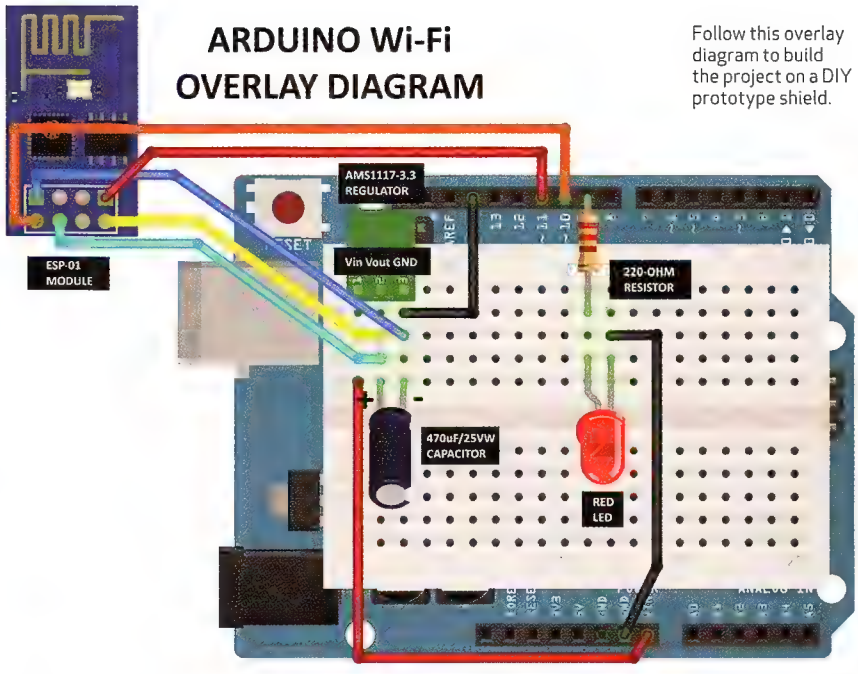
We've built the project on a DIY prototype shield plugged into a bog-standard Arduino Uno board here (you can follow the overlay diagram for details). But there's a problem – the Arduino only has one serial port (technically known as a Universal Asynchronous Receiver/Transmitter or UART for short) and we need two. We need one for the ESP8266 to communicate with the Arduino Uno and we need another for the Uno to talk to the Arduino IDE.

The trick is to incorporate a 'soft' UART using the SoftwareSerial library. A serial port is typically just two pins, one to transmit (TX) our data to a serial device and another to receive (RX) data back again. The SoftwareSerial library allows us to select any two available I/O pins on the Arduino and create a

Get the code

Download this month's source code from **www.apcmag.com/magstuff**. Unzip the file, copy the SoftwareSerial subfolder to the / libraries subfolder of your Arduino IDE and restart it. Build the circuit, load the ESPWIFI.ino code, flash it to your Arduino Uno, press the Serial Monitor button and you should see the return code.

The ESP8266 chip on this ESP-01 module is a full 802.11b/g/n Wi-Fi machine.



Follow this overlay diagram to build the project on a DIY prototype shield.

pseudo- or 'soft' serial port. Here, we're using D10 and D11.

Once the two serial ports are up, the app simply monitors the two devices: the ESP8266, to see if there's any data ready to receive; and the Serial Monitor data buffer, checking for any code you've typed in. It then processes the data and sends it in the appropriate direction.

AT CODES

The first AT command we use is 'AT+RST', which stands for 'ATtention' and 'Reset'. This tells the ESP8266 to get ready, we want it to do something and that something is reboot. Open the Serial Monitor window and you should see an initialisation string, including the device maker data. But the important bit is the 'OK' acknowledgement at the end, indicating we're good to go.

We have a number of projects in mind for the ESP8266 and one of them involves 'AT+CWLAP' (List Access Points). Type it into the Serial Monitor code line, press the Send button and the ESP8266 will list all available Wi-Fi access points (APs) within its signal radius. And the list has a bucketload of information – from the AP encryption, to its SSID or network name, its received signal strength indication (RSSI) measured in dBm (decibels referenced to one milliwatt of received power), along with its MAC address and Wi-Fi channel. The SSID and RSSI data alone give you the makings of a simple Wi-Fi Sniffer.

STATION, AP OR BOTH

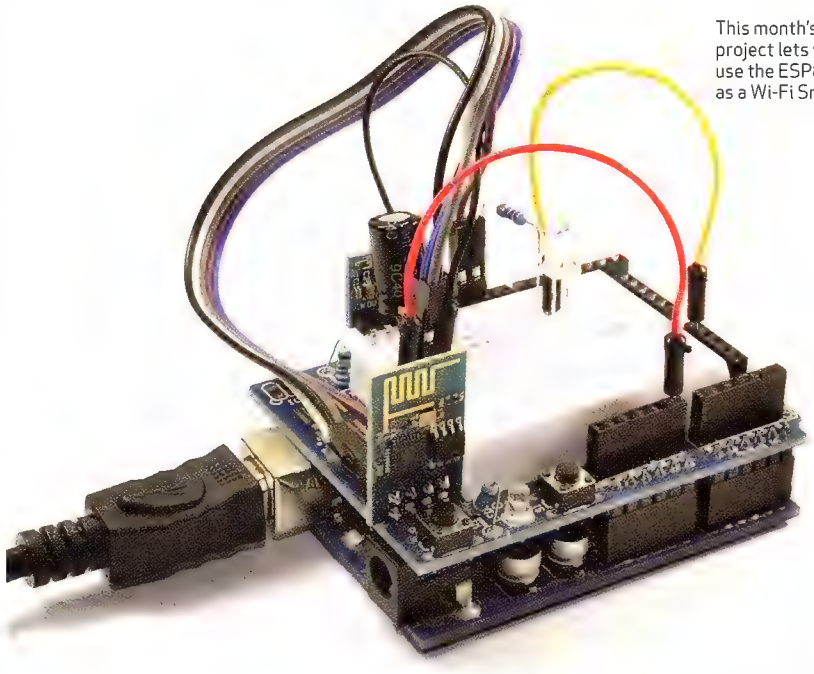
This little chip is extremely clever and can act as a Wi-Fi client and AP at the same time. You start by first running 'AT+CWMODE?' to find the current mode. Station or 'client' is Mode 1, AP is Mode 2 and both, Mode 3. You then set the mode by issuing 'AT+CWMODE=<mode number>' where <mode number> is, well, the mode number. For example, 'AT+CWMODE=3' sets up the chip to operate as both a client and AP. A more complete AT command set can be found at **tinyurl.com/p3lntvd**.

TROUBLESHOOTING

Because the ESP8266 has its own firmware, it gets updated from time to time, as noted by the first chips that arrived with a 57,600bps default serial rate, which became 9,600bps on later versions. Buy now and you should get the 9600bps version, which just means use the 'wifi.begin(9600)' codeline as-is.

The ESP-01 module has a red power LED and a blue data LED, the latter flashes when it's transmitting data. A popular mistake to avoid is to ditch the AMS1117 and just power the ESP-01 with the Arduino Uno's 3.3VDC pin instead. This method isn't recommended as the ESP8266 has a peak current draw in excess of 150mA when it's cracking on, well above the Uno's 50mA limit.

If you're seeing the command responses on the Arduino IDE Serial Monitor, you're on the right track. Next month, we'll continue by showing how to hook into your home wireless network.



This month's project lets you use the ESP8266 as a Wi-Fi Sniffer.

Java coding: claiming your inheritance

Inheritance is a major part of object-oriented programming. Darren Yates shows how it works to save you writing extra code.

Over the last few months, we've been looking at various aspects of object-oriented programming (OOP) and how it differs from other programming paradigms by concentrating your design on objects rather than procedures. Using the idea of classes, we've been able to build objects that have attributes and methods defining how the object works. For example, last month, we built a software copy of the old *Digital Derby* computer game and defined a class called 'Car', which has numerous attributes, including position parameters 'x' and 'y' to detail where on the screen frame it sat. It also has a method called 'hit' to determine whether it's hit another vehicle.

OOP is a fundamental concept any professional programmer will know intimately because it drives much of modern-day app development, from databases to games.

Coders are sometimes seen as a lazy lot – but in a very good way. No-one wants to write any more code than is absolutely necessary because more code usually leads to more mistakes, errors and bugs. So there's another important element of OOP we're looking at this month called 'inheritance'.

```
250
251     class SlowCar extends AIvehicle {
252
253         public SlowCar() {
254             setSpeed(20,10);
255         }
256     }
257
258     class CarOnComing extends AIvehicle {
259
260         public CarOnComing() {
261             x = 325;
262             setSpeed(60,20);
263         }
```

2 A new AIvehicle superclass shrinks the SlowCar and CarOnComing classes.

IS-A RELATIONSHIPS

The best way to explain any coding concept is always with code, so make sure you grab this month's source code pack from **http://apcmag.com/magstuff**. The Computer.zip file contains Computer.java. It's a fairly short program, but it'll help explain how this inheritance concept works.

We all inherit something of our parents – we've all heard people say of newborns 'she has her mother's eyes' or similar. If we try to codify that idea, we'd say a child inherits aspects or 'attributes' of its parents. This parent-child relationship idea is often used in programming and in database design, in particular.

Another way of looking at inheritance is by relationships

Get the code

Download the source code pack for this month's feature from **apcmag.com/magstuff**. Unzip it and inside the 'source code' folder, you'll find two more zip files – computer.zip and overtake2.zip. Import them into the NetBeans IDE (you can download the IDE/Java SE SDK bundle free from **oracle.com**) using File/Import Project/From ZIP and the source code should appear. Click the green Run button to run the code.

Acer's Aspire A200 is a mobile device – and a computer – at the same time.

The Digital Derby computer game modelled by our Overtake game app.

A computer shares basic specs with mobile devices and smartphones.

between objects. If we say 'a car is a vehicle', we're saying two things – first, that a car is a type of vehicle, but second, that it inherits the basic attributes of a vehicle. While it won't be apparent for now, it's also worth noting what it's not saying – it's not saying that a vehicle is a car. Any vehicle will have an engine and a number of wheels, for example, and a car has these attributes, but it also has other specific attributes that other vehicles do not – windshield wipers that you won't find on a motorcycle, for instance.

So we've talked about two basic relationship ideas here – 'is-a' and 'has-a'. A car is a vehicle. A car has wheels. The first indicates a relationship to a more generic class of object; the second represents a relationship to other objects.

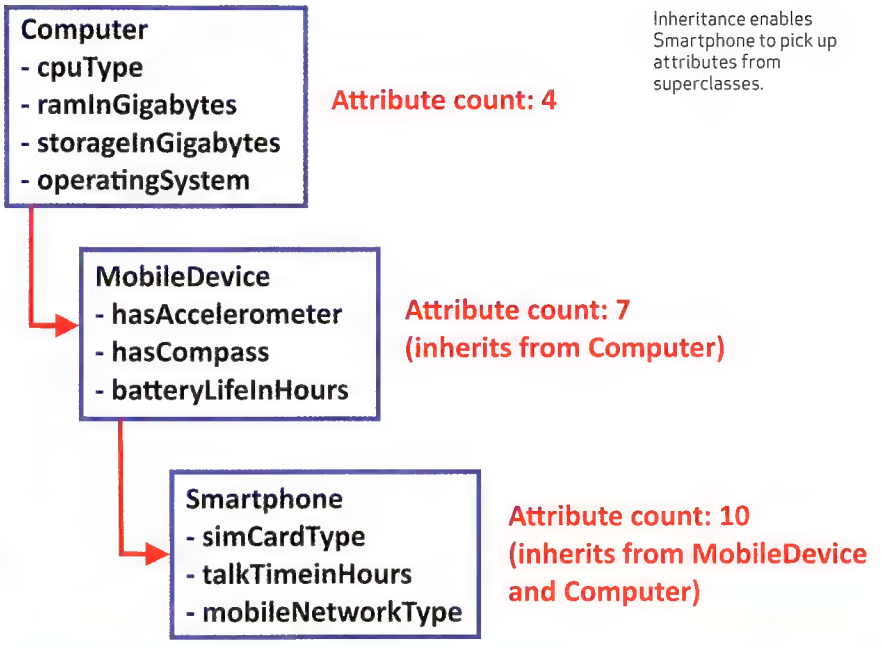
In general, almost anything that is part of an 'is-a' relationship can be modelled using this concept of inheritance.

WHAT'S IT LOOK LIKE?

Let's get a bit more practical and look at the computer.java code. We all know what a computer is – it's a device with a CPU, RAM, storage and an operating system to perform some form of programming work. So in our app, we have a class called 'Computer' with those attributes we've just mentioned – CPU, RAM, storage and OS.

But as you know, there are many different types of computers – desktops, notebooks, tablets, smartphones, mainframes, servers. They're all types of computers but importantly for us, each one shares those basic computer attributes – a CPU, RAM, storage and an OS.

Likewise, we can also say a 'Mobile Device' is a specific type of computer – it'll likely have many specific attributes such as whether or not it has a compass and accelerometer,



Inheritance enables Smartphone to pick up attributes from superclasses.

> "The idea of inheritance allows us to define 'Computer' as a base class or 'superclass' and create a new 'MobileDevice' class that includes or 'extends' that Computer class."

along with a battery life rating, for example. It still has a CPU, RAM and the rest of it, but has specific bits of its own. To model this, we could just create a new class called 'MobileDevice' with CPU, RAM, storage, OS, compass, accelerometer and battery life attributes, but we'd be duplicating attributes that are found in all computers.

The idea of inheritance allows us to define 'Computer' as a base class or 'superclass' and create a new 'MobileDevice' class that includes or 'extends' that Computer class.

Look at the Computer.java code and you'll see the code line:

```
class MobileDevice extends
Computer {
```

This tells Java exactly what we've just said – we want to create a new class 'MobileDevice' that starts by inheriting or 'extending' all of the attributes and methods found in the 'Computer' class.

But we can extend this further – a smartphone is a specific type of mobile device. It inherits all of the

Our new *Overtake2* game app uses inheritance to cut code.

Our *Overtake* game can be made better by incorporating inheritance.

Below: The Galaxy S6 is a smartphone, a mobile device and a computer.

Right: The Galaxy S6 object has a CPU type, but no direct cpuType attribute.

```
run:
Galaxy S6 CPU Type      : Samsung Exynos 7420
Galaxy S6 simCardType   : MicroSIM
Galaxy S6 accelerometer: true
Show object CPU type    : Samsung Exynos 7420
Show object CPU type    : Nvidia Tegra 2 T20
BUILD SUCCESSFUL (total time: 0 seconds)
```

```
        showData(galaxyS6);
        MobileDevice aspireA200 = new MobileDevice();
        aspireA200.cpuType = "Nvidia Tegra 2 T20";
        showData(aspireA200);
    }

    public static void showData(Computer object) {
        System.out.println("Show object CPU type    : " + object.cpuType);
    }
```

Both are 'Smartphone' objects

Subclasses can be used in place of superclasses

Polymorphism allows a subclass to be used wherever a superclass is called.

> "Why is inheritance important? Without it, the Smartphone class would need its own copies of the MobileDevice and Computer class attributes, just as the MobileDevice would also need its copies of the Computer class attributes."

basic MobileDevice attributes, but has some of its own, for example, a simCardType that a tablet may not. So we can create another class 'Smartphone' that extends 'MobileDevice':

```
class Smartphone extends MobileDevice {
```

Notice a couple of things. First, each new 'subclass' is a more specific version of its 'superclass', for example, Smartphone is a subclass of MobileDevice and MobileDevice, a subclass of Computer. Going the other way, we'd say Computer is the superclass of MobileDevice, just as MobileDevice is the superclass of Smartphone. This also highlights something else – each superclass can have many subclasses, but in many languages such as Java and C#, a subclass can have only one superclass.

Now at this point, some newbies may confuse the idea of subclasses with subsets – a subclass is not a subset of its superclass. If anything, it's the exact opposite. A car contains all the aspects of a vehicle, but has extra attributes of its own. The further down the superclass-subclass chain you go, the more specific information about an object you get – a computer can be any one of a number of diverse devices, but a smartphone is a specific type of computer with typically a larger number of attributes.

INHERITING ATTRIBUTES

So what does this all mean in practice? If you look at the main() method within the Computer class (our superclass), the first thing we do is create an object called 'galaxys6' of class type Smartphone. The next line is this:

```
galaxyS6.cpuType = "Samsung Exynos 7420";
```

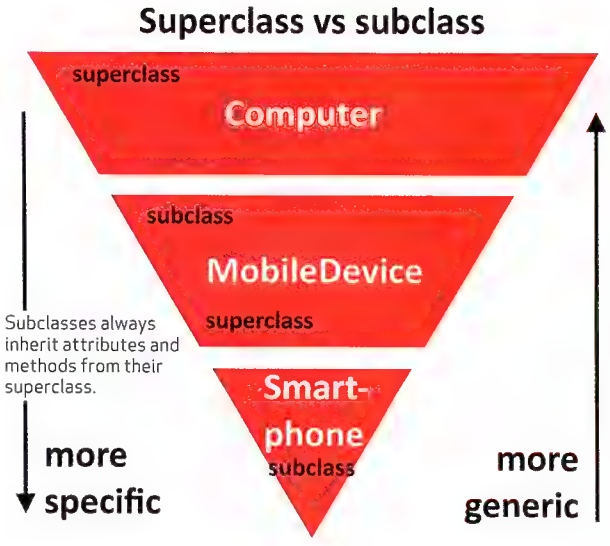
Now scroll down and look at the Smartphone class. It only has three attributes listed – simCardType, talkTimeInHours and mobileNetworkType. There's no mention of 'cpuType', yet the code works. So what's happening?

Our Smartphone class doesn't have just three attributes – it actually has 10. This is exactly where inheritance comes into play. The 'Smartphone' class extends 'MobileDevice', so Smartphone gains or 'inherits' all of the MobileDevice attributes. But also, since MobileDevice is a subclass of 'Computer', MobileDevice also inherits the Computer class attributes. That means Smartphone inherits not just the MobileDevice attributes, but also the Computer class attributes. By association, galaxyS6 has a cpuType attribute because it's inherited from the Computer class through the class 'family tree'. That's how the Smartphone class can appear to have only three attributes, but in reality has 10 – by inheriting the MobileDevice and Computer class attributes.

ONE DIRECTION

The thing to remember, however, is that, just in real life, a parent doesn't inherit from a child. Or to codify that, a superclass does not inherit the attributes of a subclass – it always works in the outward direction only.

So why is inheritance important? Without it, the Smartphone class would need its own copies of the MobileDevice and Computer class attributes, just as the MobileDevice would also need its copies of the Computer class attributes. That'd mean duplicates galore. Inheritance provides us with a form of what's often called 'code reuse', reusing earlier code so we don't have to invent the wheel every time. Essentially, it allows us to just include attributes in




```
35
36  class MobileDevice extends Computer {
37      Boolean hasAccelerometer;
38      Boolean hasCompass;
39      int batteryLifeInHours;
40
41      public MobileDevice() {
42      }
43  }
44
45  class Smartphone extends MobileDevice {
46      String simCardType = "";
47      int talkTimeInHours;
48      String mobileNetworkType;
49
50      public Smartphone() {
51      }
52  }
```

Extending classes allows you to incorporate inheritance into your code.

a class that are specific to that class, rather than clogging it up with a whole bunch of generic attributes that can be located in an appropriate superclass.

IMPROVING LAST MONTH'S CODE

Now with this new idea of inheritance under our belts, we can go back to last month's *Overtake* game and make some much needed improvements. We've included the original game code in this month's code pack (Overtake.java). If you didn't see last month, *Overtake* is a software version of the vintage computer game *Digital Derby*, where your goal is to maximise your score by driving as fast as possible and avoiding slow and on-coming traffic.

Our original code version of the game is built on three classes – Car, SlowCar and CarOnComing. It's certainly not the neatest of code and contains a fair serve of what I'd call 'slop'. There's duplication of attributes and code, unused attributes – slop. But I did give myself a tight deadline to create something from scratch, highlighting that the faster you try and code, the greater the degree of slop you produce.

More importantly, the original code has three independent classes of car. They are all doing something different, but we can still trim things down by incorporating a superclass called 'AIvehicle' and making SlowCar and CarOnComing subclasses of this superclass.

OVERTAKE2

The new version of *Overtake* is in Overtake2.zip. The benefit of inheritance here is that by making a superclass and chucking most of the class code there, we can give each subclass the same features and functions without having multiple copies and stuffing them up. The result is that there's almost no code left in both subclasses at all.

POLYMORPHISM

It's said that OOP is built on three pillars – encapsulation (which we looked at in *APC* July – see page 106), inheritance and a concept somewhat-confusingly called 'polymorphism'. Poly-what? Polymorphism, which apparently comes from ancient Greek for 'many forms'.

If we go back to our Computer.java app, we've created an instance of class 'Smartphone' called 'galaxyS6'. Now a Samsung Galaxy S6 is obviously a smartphone, but since it has a CPU, RAM, storage and an operating system, we can rightfully say a Galaxy S6 is also a computer. So 'galaxys6' is an instance of 'Smartphone', but we can also say it's an instance of 'MobileDevice' and 'Computer' – thus, it's an object of 'many forms'.

The way the concept of polymorphism works here is that anywhere in code there's a call for a 'Computer' class object, we can plug in a MobileDevice or Smartphone object as well. In more general terms, we'd say wherever you can put a superclass object, you can also throw in a subclass object.

Look at the 'showData' method inside the Computer superclass. The method header expects one parameter to be passed to it – an object of type 'Computer' called 'object'. But if you look back at the main() method, we call showData with the 'galaxyS6' object parameter, which is a Smartphone object. But again, the code works.

Because this method requires what amounts to a superclass object, we can throw any object that is a subclass of that Computer superclass. Here's another example – see the code line in the main() method:

```
MobileDevice aspireA200 =
new MobileDevice();
```

Here, we've created a MobileDevice object or instance called 'aspireA200'. But again, we've also dispatched it as a parameter to the showData() method, despite it expecting a Computer class object. Because MobileDevice is a subclass of Computer, we can use a MobileDevice class object wherever a Computer object is required. Again, our 'aspireA200' object takes on more than one form.

GIVE IT A TRY

For sure, these are complex concepts we're dealing with here. But the good news is that they're transferrable to almost any OOP-based programming language, including C# and Objective-C. (You can use C# to code Windows and Windows Phone apps, while Objective-C is the native language for iOS apps).

It's often said that once you learn how to code one OOP language, it's not that difficult to learn another. For instance, the basic concepts you use in Java are also used in C#.

Inheritance and polymorphism are fairly abstract ideas but they all add to your toolbox of tricks and provide ways of creating more efficient code.

If you're head's still spinning, this is about as abstract as we'll get in this series. But there are more mountains yet to climb – threads, networking and working with SQL databases, for example. But the bigger your apps become, the more ideas like inheritance and polymorphism can help keep your code under control. ■

downtime

» GAMES EDITED BY TROY COLEMAN

apc RECOMMENDS

US$29.99 | PC | WWW.SOMAGAME.COM

Soma

Things are not better under the sea.

Oh God, how to review *Soma* without spoilers? Interpretative dance? Nope, that's not going to work. To say almost anything about the story of Frictional Games' dark sci-fi tale would ruin it. It delves deeply into heavyweight philosophical issues around ideas of 'self' and what makes you, *you*. Don't glaze over: this isn't a dry intellectual heave of theories. It takes a couple of mind-bending concepts and weaves them into an oppressive and unsettling horror game that forces you to confront some deeply disturbing situations.

In the broadest of strokes, the story sees you trapped on an underwater research base, and desperately trying not to be. There are robots who think they're human, and tortured biomechanical growths pushing through the walls, engulfing the remains of the crew and apparently holding them in some sort of half-man, half-machine undeath.

Much of the game involves navigating uninviting corridors trying to escape. While the trailers pushed a stealth/horror vibe, avoiding monsters is only a small part of the mix, and actually its weakest facet. Instead of predatory fiends hunting you down, these creatures are lumbering patrollers, mindlessly wandering a set route in a small area – usually blocking your path to either a thing or a door you need to reach. The solution is always to lead them away, then loop back, and the predictable behaviour means it's an element that's not as scary as we'd hoped, despite a few jumpy moments.

There are also only five or six such encounters in the whole ten-hour play time. The weight of the experience really comes from exploring both the base and the story – piecing together what's actually happened, or solving puzzles to progress. There's a marvellously tactile feel to the world, with the right trigger and stick used to grab and manipulate objects. It's a simple gimmick but there's something satisfying about manually pulling open drawers and yanking on wires. This physicality is reflected too in the game's refreshingly grounded puzzles, each based in real-world logic. This is a game with no pings, updating objective markers, or any other traditional guidance, meaning you actually have to look around and figure out what you need to use.

One situation involves a computer requesting a login that you eventually get from a security card found on a body. The game doesn't tell you any of this, or even react when you find computer or card. Only when you put the two together – remembering the number in your actual head – does something happen. It can make the first few hours slow while your brain adjusts, and there are times when you're not sure if you're on the right track, but it can be incredibly satisfying when you realise you are.

The real pay-off to *Soma*, though, is completing its story. As you push deeper into all the things we can't really talk about, it gets brilliantly unpleasant, worming concepts and realisations into your brain that don't play well with your happy place. At least one decision made us actually detest the developer for forcing it on us, while the final resolution is the kind of thing that will haunt you for years to come. In a good way.

■ Leon Hurley

Verdict

Slow to start with, but ultimately a rewarding, dark and unsettling exercise in conceptual horror.

★★★★

Fights against major villains always demand clever Toy Pad manipulation.

$169.99 (STARTER PACK) | XO, PS4, XBOX360, PS3 | WWW.LEGO.COM/DIMENSIONS

Lego Dimensions

Parents everywhere are going to be bricking it.

How deep are your pockets? That's the question you need to be asking yourself, because *Lego Dimensions* isn't just a single game in a box with a few bonus Lego toys – it's an expansive Lego platform with a vast range of dangerously appealing add-on elements, and going in completely blind will trip up the unprepared.

It's important to address this right away because while its basic Starter Pack does indeed contain hours and hours worth of gaming in its own right (not to mention actual Lego to build), *Lego Dimensions* isn't shy about asking you to spend again.

In true Lego gaming fashion, different characters and vehicles have different skills, which will let you complete various puzzles as you progress through the adventure. But unlike those past Lego titles you know and love, you unlock these characters and accessories in *Lego Dimensions* by buying the actual models themselves, building them, and scanning them into the game. Once the opening is complete, Batman, Gandalf and Wyldstyle are whisked away to the land of Oz for the game's first level. It's a fantastically realised place filled with soaring simians, a lemon block path and a side-splitting scarecrow gag that typifies *Lego Dimensions*' excellent wit. But I move no more than a few steps before encountering my first obstacle: a blockade of silver bricks that can be destroyed by a bunch of different characters not in the Starter Pack. Thankfully, I have the *Wizard of Oz Wicked Witch Fun Pack* so can press on into that new area, but a few steps in, I need another character to activate something else.

Again, that's not a problem as I own him, too, but a few steps beyond that I need characters who aren't yet available, before then encountering a puzzle that requires a Ninjago minifig. It really sours the journey, because while *Lego Dimensions* isn't among TT Games' best 'pure' *Lego* games, it is a lot of fun.

Playing with actual Lego adds an awful lot to the experience, and the Toy Pad proves to be quite the headscratcher as I'm forced to bounce minifigs around its flashing panels to escape boss attacks, trigger elemental spells and warp my in-game toys to different parts of the level. The physical nature of placing, removing and – when it comes to upgrading my rides – rebuilding my toys, is hugely rewarding. Deeper into the game, when levels open up somewhat and I start to explore the sandbox side-worlds, things click even more, and all the while the gags that sprout from the IP mix mean I'm always left grinning.

Yet it could have been so much more. More restraint when it came to the 'paywall' frequency and more creativity to break the small area/boss/small area/boss pattern could have made this an instant classic. Instead, it's a fun first toys-to-life attempt that's too blunt about wanting extra cash.

Matthew Pellett

Verdict

A playful and genuinely funny outing boasting exceptional licenses, a crazy story and wonderful toys.

★★★½☆

NBA 2K16

Still king of the court.

FROM $79.95 | XO, PS4, XBOX360, PS3 | WWW.2K.COM

As incredible-looking player models squeak around shiny floors, grimacing for dunks and dripping sweat, it's clear no sports experience comes close to NBA 2K16's presentation. And it extends past visuals: a studio roundtable discusses key points ahead of the game, talking heads give soundbites during breaks, and there are full halftime performances from cheerleaders.

This year, with the help of joint-maker Spike Lee, 2K doubles down on off-the-court shenanigans. A full story mode containing mo-capped cinematics follows your hopeful from high school to the big time, courted by colleges and wooed by sponsors. Since you only have to focus on one player, MyCareer is the perfect entry point for novices.

It's a different matter outside of career mode. Where EA uses the excellent FIFA Trainer to teach techniques, NBA 2K16 sticks to short and plain tutorial videos narrated by mumbling stars. Still, if you've played any recent game in the series, you'll appreciate improvements to physics and player movement — both are more fluid and convincing. Options are vast, too. You can play one-on-one on concrete courts, customise jerseys for your created team, go for glory as GM by maintaining media relationships and setting hot dogs prices, and even design your own trainers.

From the banging 50-song soundtrack to an in-game shop flogging gold watches for your player, NBA 2K16 simulates not only a sport, but a lifestyle. **Ben Griffin**

FROM $89.95 | PS4, XO, PC, PS3, 360 | WWW.EASPORTS.COM/AU

FIFA 16

Blatter the devil you know.

You know those odd mini-tournaments that run in the off months when there's no World Cup or European Championships to distract from the horror that is your particular club's dire transfer dealings? The ones sponsored by car manufacturers or pharmaceutical giants eager to bask in the glow of the beautiful game? This game has those.

In fact, for anyone who leaps straight into any of *FIFA*'s career modes, those vacuous tournaments will be the first competitions of any kind they'll play. In the real world, such events are nothing but a bit of promo-focused fluff. In *FIFA 16*, they're an example of the small steps the franchise takes with each iteration not only to simulate the on-pitch action, but also the world of football as a whole.

FIFA rarely takes bold steps forwards, with EA instead opting to gradually re-shape its mould with each release rather do anything radical. From the outset, it's worth pointing out that that's exactly what's happened here: *FIFA 16* doesn't reinvent the wheel, with much of the game indistinguishable from last year's effort.

There are two areas on the pitch that feel notably different, however, with shots on goal one component that the dev team has moved to refine within its latest offering. To put it simply, to score in *FIFA 16*, you need to give that button a good, hard press. Tapping it lightly will, nine times out of ten, see the ball simply roll into the keeper's hands.

Jostling for the ball has also been rebalanced, with holding onto it – even when pushing off your rival with your arm – far trickier than it's felt in previous releases. These changes will undoubtedly feel quite alien to veteran *FIFA* aficionados at first, but when fused with subtle changes to the game's AI – an utterly realistic tendency for teams to lose the ball by making the occasional unfortunate pass a particular highlight – what results is a more lifelike, convincing take on the average game of football.

Off the pitch, much of the advancements in *FIFA 16* are largely cosmetic – shifts that don't make too much difference to your performance on the field, but further assert the notion of EA's series being the digital home of the world's most popular sport.

Of course, whatever *FIFA 16* does or doesn't do, gamers will inevitably want to line it up against *Pro Evolution*. Predictably, there's no great attempt to move in on *PES* territory here with EA seemingly content with *FIFA*'s comparatively modest scheme, even if the two are arguably as close as they ever have been when it comes to on-the-pitch action. Arguably, this isn't as big a step forward as the PS4 and Xbox One version of *FIFA 15*, but it is nevertheless another modest advance on what the series has served up before. Established fans are unlikely to be blown away by enduring evolution rather than revolution of the *FIFA* model as showcased here, but to stick the boot into EA for once again playing safe would be to denigrate the overall quality of the game. Like lavishing praise on Luis Suarez, talking up *FIFA 16* may not be something many are comfortable with doing, but the latest version of EA's most enduring franchise is one of the best to date, and a game that further pulls *FIFA* clear of *Pro Evo* at the top of the table.

■ Keith Andrew

Verdict

Not a massive step forward, but EA's evergreen series remains well ahead of the competition.

The in-game camera comes with an array of lenses and filters – you can now record animated GIFs to share online.

$69.95 | PS4 | TEARAWAY.MEDIAMOLECULE.COM

Tearaway Unfolded

The Vita classic gets a second life on PS4.

Somewhere on a wall in Media Molecule's HQ will be a cluster of Post-Its. It's a common sight in dev studios, ideas roughed out in sticky notes that can be moved around or thrown away without disrupting the rest of the plan. 'Tickle bad guy'. 'Gopher basketball'. 'Paper aeroplane selfie'. If you didn't know they formed the outline for a game you'd assume they were the scattered, multicoloured ravings of a lunatic.

Lunacy, however, is something Media Molecule does exceptionally well. There was plenty of it in the original *Tearaway* on Vita, where the studio made brilliantly creative use of all the system's weird little features – its front and rear touch, its dual cameras and gyroscopes. And there's even more of it here, as MM attempts to do the same for DualShock 4 as it did for Sony's handheld console.

Rather than build a new title around new ideas, Media Molecule has chosen to bring the original across wholesale, tweaking mechanics where the DualShock 4 is up to the task, and adding in new ones to replace those that can't make the transition.

So you still use touch to activate drum pads that catapult the protagonist (Iota if you choose to play as a boy, or Atoi for a girl) into the air. But instead of using Vita's rear touch, you press the DS4's touchpad. It's also used to generate gusts of wind, and to power the cutting-mat sections, where you make rough papercraft objects to add to the world. Since it's just one fifth the size of Vita's touchscreen, creation is an awkward process. The job can be moved to a second screen – a phone, tablet or even Vita, through the PlayStation app – with better results, but the sense that you are holding a world in your hands, so central to the Vita game's magic, is lost the instant you put down the controller to grab something else.

At least the new additions have the DualShock 4's forgotten features at their core. The light bar powers Guiding Light, where a press of R2 projects a beam on-screen that hypnotises bad guys, suckering them into flinging themselves into walls or off ledges. Grab a creature, tilt the pad towards you and push Square and Atoi or Iota will fling the critter out of the screen and into the DualShock 4.

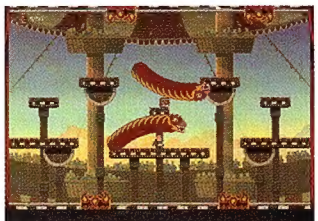
It's playful stuff throughout, but the new additions are no substitute for the sight of a rendered finger bursting through the game-world's floor when you pressed Vita's rear panel, or the way its front camera showed a close-up of your smiling face gazing down from the sky. *Unfolded* just can't quite match up to its handheld counterpart, and much of that is down to the fact that it's essentially the same game stripped of some of what made it so special. A wayward camera and wobbly framerate hardly helps matters, either. Newcomers will find plenty here to love, but despite the new ideas, old hands will feel like they've seen it all before, and better.

■ Nathan Brown

Verdict

Charming stuff once again from Media Molecule, but the PS4 version can't rekindle its handheld magic.

★★★½☆



Penarium

"The Sadistic Circus Extravaganza!"

FROM US$9.95 | XBI, PS4, PC
WWW.PENARIUM.COM

Who hasn't heard the old story? A child, bored with his humdrum farm life, runs away to join the circus, only to find himself imprisoned in an arena, avoiding a series of whimsical traps that have the express purpose of killing him for the crowd's amusement. What, you mean you haven't heard that classic tale?

Penarium is that arena, and surviving the nightmarish circus is harder than it sounds. You're able to jump or double jump away from danger and, um... that's it, but *Penarium* wrings a lot of entertainment out of simple concepts. Danger comes at you from every direction — in a variety of combinations — and one of the hardest things to master is subduing your own panicked instinct to jump away from one hazard face first into another.

Mercifully, reload time is as instant as your grisly death, so even if you fail in quick succession it feels more challenging than frustrating. Repetition will eventually take hold, however. You may have a psychotic ringmaster to keep you entertained, but there are still only so many ways to die. Yet even then there's hope; its endless arcade and multiplayer modes keeping you interested for longer.

Penarium's quirky design — modelled after retro arcade games — and dark influences definitely give it impressive razzle-dazzle, but not enough to warrant unlimited repeat visits. Which is strange, since a real life circus where children compete to stay alive would probably be a massive hit on reality TV.

■ Alice Bell

Selfies that kill

Snapper vs snapper: selfies responsible for more deaths per annum than shark attacks.

Turns out you're more likely to die taking a photo of yourself than you are by diving into the ocean where sharks live. This year, twelve people have died whilst taking a photo of themselves, while eight people have been killed by what tabloid media likes to call 'the killing machine of the ocean'. The causes of those selfie deaths? Falling (say, down stairs) and being hit by trains, mostly.

The problem (possibly stupidity, as people are more concerned with taking a photo of themselves rather than their personal safety) has caused one park in Denver, Colorado, to close as visitors keep taking selfies with bears, while Disneyland has banned selfie sticks, with a spokesperson for the theme park saying they are "a growing safety concern".

Internet-connected kettles leak passwords

HUBBLE, BUBBLE, BOIL AND TROUBLE.

A security and penetration testing organisation has hacked a series of networked kettles across London, revealing the devices can leak home Wi-Fi passwords. Yes, the Internet of Things now incudes kettles, specifically the iKettle, which can be controlled using an app on iOS or Android to save vital seconds when boiling water for a cuppa.

Using special equipment including a directional antennae and networking gear, plus social engineering data, Ken Munro from Pen Test Partners says it's simple to hack in and take control. "If you haven't configured the kettle, it's trivially easy for hackers to find your house and take over your kettle," Munro says. "Attackers will need to setup a malicious network with the same SSID but with a stronger signal that the iKettle connects to before sending a disassociation packet that will cause the device to drop its wireless link."

British spy agency says complex passwords 'pointless'

COINCIDENTALLY, WAS ALSO SPYING ON UK CITIZENS.

You may've heard of GCHQ before — former NSA contractor Edward Snowden told the world the agency was collecting online and telephone data from British citizens before he famously went into exile in 2013.

Now, in a new report, the spy agency has said that creating overly long or complex passwords does little to deter professional hackers, and only creates confusion for everyday-users' lives.

In its list of recommendations, GCHQ does make some sensible suggestions, such as changing default passwords and not storing password lists in plain text files. Simple three-word passwords may also be effective, and while it admits that software designed to manage a series of passwords can be helpful, it claims "they are not impregnable and are an attractive target for attackers".

APC's recommendation? Don't revert to 'password1' or 'qazwsx' — and do grab and use a password manager, like the ones we've reviewed from page 60.

China gets an official Pepsi phone

P1 SMARTPHONE TO BE THE CHOICE OF A NEW GENERATION?

The world's second-biggest cola brand is branching out beyond beverages. And rather than wrapping its name around an established smartphone, Pepsi is selling its own phone in the Chinese market. Customers in the East are now able to buy a 5.5-inch, 1080p smartphone running Android 5.1 called the Pepsi P1 — it costs 1,299 Yuan, or approximately AU$280. The price is right, especially when you consider its other specs: all-metal body that's 7.7mm thick, 1.7GHz quad-core ARM MT6592 processor, 2GB memory and 16GB of internal storage, with a 3,000mAh battery. But what makes it a Pepsi phone, other than the red, blue and white colours on the body? Right now, we're unsure… but who can resist the magnetic allure of conspicuous branding, right? ■

msi®
HEROES OF THE STORM™
GAMING G SERIES
BE A HERO WITH
MSI GAMING NOTEBOOK
-OPTIMIZED AND BATTLE-TESTED-

MSI ANZ FB

WORLD'S FIRST

WITH THE LATEST 6TH GEN.
INTEL® CORE™ i7-6700HQ PROCESSOR.

intel CORE i7 inside™

| WINDOWS 10 HOME |

Start from : AUD$2,000

| NVIDIA GTX 980M / 970M GRAPHICS | SUPER RAID 4 | PCI-E GEN.3 X4 SSD |

| SABRE HiFi | KILLER DOUBLE SHOT PRO WITH SHIELD | SUPER PORT | DDR4-2133 | USB3.1 |

INTEL INSIDE®. EXTRAORDINARY PERFORMANCE OUTSIDE.

WHERE TO BUY

NSW	Capitol Computer	(02) 9281 8890	www.capitolcomputer.com.au
	Techbuy	(02) 9648 1818	www.techbuy.com.au
	Mwave	1300 727 446	www.mwave.com.au
	Kong Computers	1300 159 272	www.kongcomputers.com
	JW Computers	(02) 9726 2818	w.com.au
VIC	Tecs	(03) 9602 3499	www.tecs.com.au
	Scorptec Computers	(03) 9249 6000	scorptec.com.au
	PC Case Gear	(03) 9560 2122	www.pccasegear.com
	Centrecom	(03) 8311 7600	www.centrecom.com.au
QLD	Umart	(07) 3369 3928	www.umart.com.au
	Computer Alliance	(07) 3421 3200	www.computeralliance.com.au
	GameDude Computers	(07) 3387 1500	www.gamedude.com.au
WA	Affordable laptops	(08) 9536 8500	www.affordablelaptops.com.au
	PLE Computers	(08) 9309 4771	www.ple.com.au/
	Austin Computers	(08) 9202 0100	austin.net.au
SA	IT Warehouse	(08) 8296 3211	www.itwarehouse.com.au
New Zealand	Just Laptops	0800 58 78 52	www.justlaptops.co.nz
	Computer Lounge	(09) 368 4818	www.computerlounge.co.nz
	Playtech	(09) 415 1020	www.playtech.co.nz

GAMING.MSI.COM

Intel, the Intel Logo, Intel Inside, Intel Core, and Core Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

msi®

Windows 10

Windows 10. Do great things.

intel CORE™ i7 inside™

SEE MORE. GAME BETTER.

GAMING G SERIES

GAMING All-in-One PC / GAMING Desktop PC

Model Name	Gaming27	NIGHTBLADE MI2	NIGHTBLADE X2
Operation System	Windows10 Home	Windows10 Home	Windows10 Home
System Memory	DDR4 2133MHz up to 64GB	DDR4 2133MHz up to 16GB	DDR4 2133MHz up to 16GB
CPU	Intel® Core™ i7 Processor	Intel® Core™ i7 Processor	Intel® Core™ i7 Processor
VGA	NVIDIA GeForce GTX 980M 8GB GDDR5	Up to NVIDIA GeForce GTX970 4GB GDDR5	Up to NVIDIA GeForce GTX980 8GB GDDR5
Storage	2 x M.2 PCIE +1 x 3.5" HDD	1 x M.2 PCIE + 2 x 3.5" HDD + 1 x 2.5" HDD	2 x M.2 PCIE + 1 x 3.5" HDD + 2 x 2.5" HDD

The faster the better. It's time for MSI Gaming PC with Intel Inside® and Windows® 10!

© 2015. MSI is a registered trademark of Micro-Star Int'l Co.Ltd. All other trademarks are the property of their respective owners. Product features may vary by market, please check your local dealer for specification. Specs and features vary per model. Check with your local reseller for details.

GAMING.MSI.COM